

M208

Pure mathematics

Book E

Group theory 2

This publication forms part of an Open University module. Details of this and other Open University modules can be obtained from Student Recruitment, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)300 303 5303; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2019.

Copyright © 2019 The Open University

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Barnard's Inn, 86 Fetter Lane, London EC4A 1EN (website www.cla.co.uk).

Open University materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or retransmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using L^AT_EX.

Printed in the United Kingdom by Hobbs the Printers Limited, Brunel Road, Totton, Hampshire, SO40 3WX.

Contents

| | | |
|-------------------------------|------------------------------------|-----------|
| Unit E1 | Cosets and normal subgroups | 1 |
| Introduction to Book E | | 3 |
| Introduction | | 3 |
| 1 | Groups | 4 |
| 1.1 | Definition of a group | 4 |
| 1.2 | Permutation groups | 12 |
| 1.3 | Symmetry groups | 19 |
| 1.4 | Subgroups | 22 |
| 2 | Matrix groups | 27 |
| 3 | Group structures | 36 |
| 3.1 | Order of a group element | 36 |
| 3.2 | Cyclic subgroups | 41 |
| 3.3 | Cyclic groups | 43 |
| 3.4 | Isomorphic groups | 45 |
| 4 | Cosets | 52 |
| 4.1 | Left cosets | 53 |
| 4.2 | Right cosets | 62 |
| 4.3 | Cosets in additive groups | 69 |
| 5 | Normal subgroups | 75 |
| Summary | | 80 |
| Learning outcomes | | 80 |
| Solutions to exercises | | 81 |

| | | |
|----------------|---|------------|
| Unit E2 | Quotient groups and conjugacy | 97 |
| | Introduction | 99 |
| 1 | Quotient groups | 99 |
| 1.1 | What is a quotient group? | 99 |
| 1.2 | Quotient groups of infinite groups | 115 |
| 1.3 | Simple groups (optional) | 124 |
| 2 | Conjugacy | 129 |
| 2.1 | Conjugacy in symmetric groups | 129 |
| 2.2 | Conjugacy in general | 134 |
| 2.3 | Conjugacy classes | 138 |
| 3 | Normal subgroups and conjugacy | 146 |
| 3.1 | Normal subgroups and conjugates | 147 |
| 3.2 | Conjugate subgroups | 151 |
| 3.3 | Normal subgroups and conjugacy classes | 155 |
| 3.4 | Proofs of the theorems characterising normality | 161 |
| 4 | Conjugacy in symmetry groups | 164 |
| 4.1 | Conjugacy and geometric type | 164 |
| 4.2 | Finding conjugacy classes of finite symmetry groups | 174 |
| 5 | Conjugacy in matrix groups | 180 |
| 5.1 | Conjugate subgroups in matrix groups | 180 |
| 5.2 | Normal subgroups in matrix groups | 185 |
| | Summary | 188 |
| | Learning outcomes | 188 |
| | Solutions to exercises | 189 |

| | |
|---|------------|
| Unit E3 Homomorphisms | 207 |
| Introduction | 209 |
| 1 Isomorphisms and homomorphisms | 209 |
| 1.1 Isomorphisms | 209 |
| 1.2 Homomorphisms | 222 |
| 1.3 Properties of homomorphisms | 231 |
| 2 Images and kernels | 239 |
| 2.1 Image of a homomorphism | 239 |
| 2.2 Kernel of a homomorphism | 247 |
| 2.3 Finding images and kernels | 253 |
| 3 The First Isomorphism Theorem | 261 |
| 3.1 Cosets of the kernel of a homomorphism | 261 |
| 3.2 The First Isomorphism Theorem | 265 |
| 3.3 Infinite quotient groups of domain groups by kernels (optional) | 272 |
| Summary | 276 |
| Learning outcomes | 276 |
| Solutions to exercises | 277 |

| | | |
|----------------|--|------------|
| Unit E4 | Group actions | 291 |
| | Introduction | 293 |
| 1 | Group actions | 293 |
| 1.1 | What is a group action? | 293 |
| 1.2 | Actions of groups of symmetries | 303 |
| 1.3 | Actions of groups of numbers | 311 |
| 1.4 | Actions of matrix groups | 314 |
| 2 | Orbits and stabilisers | 317 |
| 2.1 | Orbits | 317 |
| 2.2 | Orbits of group actions on \mathbb{R}^2 | 325 |
| 2.3 | Stabilisers | 330 |
| 2.4 | Stabilisers of group actions on \mathbb{R}^2 | 335 |
| 3 | The Orbit–Stabiliser Theorem | 340 |
| 3.1 | What is the Orbit–Stabiliser Theorem? | 340 |
| 3.2 | Left cosets of stabilisers | 341 |
| 3.3 | Groups acting on groups | 347 |
| 4 | The Counting Theorem | 352 |
| 4.1 | Counting problems involving symmetry | 352 |
| 4.2 | Fixed sets | 356 |
| 4.3 | The Counting Theorem and its use | 365 |
| 5 | Group actions and groups of permutations (optional) | 378 |
| | Summary | 384 |
| | Learning outcomes | 384 |
| | Solutions to exercises | 385 |
| | Acknowledgements | 403 |
| | Index | 405 |

Unit E1

Cosets and normal subgroups

Introduction to Book E

You met many of the basic ideas of group theory in Book B *Group theory 1*. This book builds on that material and introduces you to more advanced group theory. You will learn more about how group theory reveals links and similarities in concepts that seem unrelated, giving us a greater understanding of these concepts. You will also see examples of how group theory can simplify problems that at first sight appear prohibitively complicated, and so make it possible to solve them.

The mathematics that you will cover in this second group theory book is more abstract than that in the first book, and many students find it more challenging. However, do not let that put you off – being challenged should be an enjoyable part of learning mathematics, and it enables you to meet some quite powerful and beautiful group theory.

To avoid this book being *too* challenging, though, you must make sure that you have a really sound working knowledge of the material covered in the first group theory book, Book B, which forms a foundation for this second book. To help you achieve this, this second book of group theory includes revision of the main ideas and techniques that you will need from the first book. You should work carefully through all the revision material, most of which is in the first unit. Doing this will also give you a useful start on your exam revision.

The ideas that you have already met in Book B are covered much more concisely here than in Book B, so if you find that you need more detail on a topic then you should consult the original coverage of it in Book B. Most of the results from Book B are stated here without proof, as they have already been proved in Book B.

The second unit in this book, Unit E2, is more substantial than the other three units, so you should expect to spend more time studying it.

Introduction

Sections 1 and 3 of this unit, which together constitute about half of the unit, are devoted to revision of some of the important ideas from Book B. They will give you the grounding that you need before you go on to the more abstract group theory later in the book. These sections also include some interesting examples of groups that you have not met before.

The other three sections cover new topics. Section 2 introduces *matrix groups* – groups whose elements are matrices – which will be used frequently in this book. Section 4 introduces the idea of *cosets*, which are subsets of a group related to a particular subgroup. This work leads in Section 5 to the notion of a *normal subgroup*, which is a crucial concept in group theory: normal subgroups allow us to ‘break down’ groups into simpler groups. Both cosets and normal subgroups will be important throughout the rest of this book.

1 Groups

In this first section you will revise the definition of a group and some basic properties of groups, and go on to revise permutation groups, symmetry groups and subgroups.

1.1 Definition of a group

In mathematics, there are many situations in which we have a set together with a means of combining any two elements of the set. For example, we might have one of the following.

- The set of all real numbers, with addition. We can use addition to combine any two real numbers: for instance, $2.1 + 3.7 = 5.8$.
- The set of all symmetries of the square, with function composition. We can use function composition to combine any two symmetries of the square. For instance, if the symmetries of the square are labelled as shown in Figure 1, then $a \circ b = c$.

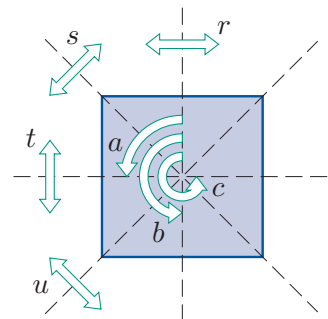


Figure 1 The symmetries of the square

A means of combining any two elements of a set is called a **binary operation** defined on the set. If a set and a binary operation defined on the set together possess the four standard properties given in the box below, then the set and binary operation are said to form a *group*.

Definition

Let G be a set and let \circ be a binary operation defined on G . Then (G, \circ) is a **group**, and we also say that G is a **group under** \circ , if the following four **group axioms** hold.

G1 Closure For all g, h in G ,

$$g \circ h \in G.$$

G2 Associativity For all g, h, k in G ,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

G3 Identity There is an element e in G such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for \circ on G .)

G4 Inverses For each element g in G , there is an element h in G such that

$$g \circ h = e = h \circ g.$$

(The element h is an **inverse element** of g with respect to \circ .)

This definition is illustrated in the worked exercise below. When you apply it you may assume without proof that the following binary operations are associative. (You saw that matrix multiplication is associative in Corollary C44 at the end of Subsection 3.1 of Unit C3.)

Standard associative binary operations

- Addition
- Multiplication
- Modular addition
- Modular multiplication
- Matrix addition
- Matrix multiplication
- Function composition



Worked Exercise E1

Determine which of the following are groups.

- (a) (\mathbb{Z}, \times) (b) $(\mathbb{Z}, +)$

Solution

- (a) We consider each axiom in turn.

 To show that a group axiom holds, we must give an algebraic argument that applies to all group elements (though we can assume that axiom G2 holds if the group operation is one of the standard associative binary operations). To show that a group axiom does *not* hold, we must give a counterexample. 

G1 Closure

For all $m, n \in \mathbb{Z}$,

$$m \times n \in \mathbb{Z},$$

so \mathbb{Z} is closed under multiplication.

G2 Associativity

Multiplication of numbers is associative.

G3 Identity

We have $1 \in \mathbb{Z}$, and for all $n \in \mathbb{Z}$,

$$n \times 1 = n = 1 \times n.$$

So 1 is an identity element for \times on \mathbb{Z} .

G4 Inverses

The element 2 is in \mathbb{Z} , but it has no inverse with respect to multiplication in \mathbb{Z} , since there is no element $n \in \mathbb{Z}$ such that

$$2 \times n = 1 = n \times 2.$$

Thus axiom G4 fails.

Hence (\mathbb{Z}, \times) is not a group.

(b) Again, we consider each axiom in turn.

G1 Closure

For all $m, n \in \mathbb{Z}$,

$$m + n \in \mathbb{Z},$$

so \mathbb{Z} is closed under addition.

G2 Associativity

Addition of numbers is associative.

G3 Identity

We have $0 \in \mathbb{Z}$, and for all $n \in \mathbb{Z}$,

$$n + 0 = n = 0 + n.$$

So 0 is an identity element for $+$ on \mathbb{Z} .

G4 Inverses

For each $n \in \mathbb{Z}$, we have $-n \in \mathbb{Z}$ and

$$n + (-n) = 0 = -n + n.$$

So each element n in \mathbb{Z} has an inverse element in \mathbb{Z} with respect to addition.

Since all four axioms hold, $(\mathbb{Z}, +)$ is a group.

Although the solution to Worked Exercise E1(a) proceeds by considering all the group axioms systematically until one is found to fail, simply demonstrating that *any one* axiom fails is enough to show that a set and binary operation do not form a group.

Exercise E1

Let $A = \{5k : k \in \mathbb{Z}\} = \{\dots, -10, -5, 0, 5, 10, \dots\}$.

By using the group axioms, determine which of the following are groups.

(a) $(A, +)$ (b) (A, \times)

The next exercise involves a group that you have not met before but which will be used later in this book. The binary operation of this group is defined using the idea of the *fractional part* of a real number.

The **fractional part** of a real number x , denoted by $\text{frac}(x)$, is given by

$$\text{frac}(x) = x - \lfloor x \rfloor,$$

where $\lfloor x \rfloor$ is the integer part of x (the largest integer that is less than or equal to x).

For example,

$$\text{frac}(1.2) = 1.2 - 1 = 0.2,$$

$$\text{frac}(3.9) = 3.9 - 3 = 0.9,$$

$$\text{frac}(5) = 5 - 5 = 0,$$

$$\text{frac}(-2.8) = -2.8 - (-3) = 0.2.$$

Essentially, $\text{frac}(x)$ is equal to 0 if x is an integer, and is equal to the distance from x to ‘the next integer down’ otherwise, as illustrated in Figure 2. So it is always a number in the interval $[0, 1)$.

The binary operation $+_1$ is defined on the interval $[0, 1)$ by

$$x +_1 y = \text{frac}(x + y).$$

For example,

$$0.9 +_1 0.7 = \text{frac}(0.9 + 0.7) = \text{frac}(1.8) = 0.8.$$

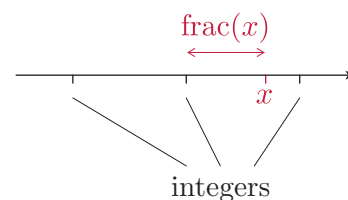


Figure 2 The fractional part of a real number x

Exercise E2

Given that the binary operation $+_1$ defined above is associative on the interval $[0, 1)$, show that $([0, 1), +_1)$ is a group.

(If you want a challenge, try showing also that $+_1$ is associative on $[0, 1)$. A solution to this is provided at the end of the solution to this exercise.)

A group (G, \circ) that has the additional property that

$$g \circ h = h \circ g \quad \text{for all } g, h \text{ in } G$$

is called an **abelian** (or **commutative**) group. A group that is not abelian is **non-abelian**.

The group $(\mathbb{Z}, +)$, from Worked Exercise E1(b), is an example of an abelian group, since $a + b = b + a$ for all $a, b \in \mathbb{Z}$. In fact, any group whose elements are numbers and whose binary operation is addition or multiplication is an abelian group, since $a + b = b + a$ and $a \times b = b \times a$ for all numbers a and b . In contrast, a group whose binary operation is function composition or matrix multiplication may be either abelian or non-abelian.

An **infinite** group is one with infinitely many elements. So, for example, the group $(\mathbb{Z}, +)$ is an infinite group. A **finite** group is one with a finite number of elements. If a finite group (G, \circ) has n elements, then we say that it is a group of **order** n , and we write $|G| = n$.

The infinite groups of numbers in the box below occur frequently. Remember that $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$ and $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Some standard infinite groups of numbers

The following are groups:

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +), \\ (\mathbb{Q}^*, \times), \quad (\mathbb{R}^*, \times), \quad (\mathbb{C}^*, \times).$$

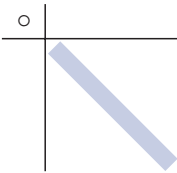


Figure 3 The main diagonal of a Cayley table

When we are working with a binary operation \circ defined on a small finite set, we often display the composites given by \circ in a **Cayley table**. For each x and y in the set, we enter the composite $x \circ y$ in the Cayley table in the row labelled x and the column labelled y . We can use a Cayley table to help us check the group axioms, as described in the box below (recall that the *main diagonal* of a Cayley table is the diagonal shown in Figure 3). The construction of a Cayley table and its use to check the group axioms are demonstrated in the next worked exercise after the box.

Using a Cayley table to check the group axioms

Let G be a finite set and let \circ be a binary operation defined on G . Then (G, \circ) is a group if and only if the Cayley table for (G, \circ) has the following properties.

- G1 Closure** The table contains only elements of the set G ; that is, no new elements appear in the body of the table.
- G2 Associativity** The operation \circ is associative.
(This property is not easy to check from a Cayley table.)
- G3 Identity** A row and a column labelled by the same element repeat the table borders. This element is an identity element, e say.
- G4 Inverses** Each row contains the identity element e , occurring either on the main diagonal or symmetrically with another occurrence of e , with respect to the main diagonal (see Figure 4). For each such occurrence of e , the corresponding elements in the table borders are inverses of each other.

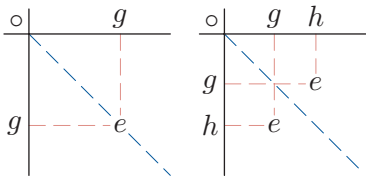


Figure 4 Occurrences of the identity element indicating inverse elements

Remember also that a finite group is abelian if and only if its Cayley table is symmetric with respect to the main diagonal.

A Cayley table of a group is called a **group table**.

Worked Exercise E2

Construct a Cayley table for the set $G = \{1, 3, 7, 9\}$ under multiplication modulo 20. Hence show that (G, \times_{20}) is a group.

Solution

The Cayley table is as follows.

| \times_{20} | 1 | 3 | 7 | 9 |
|---------------|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

We consider each axiom in turn.

G1 Closure

Every element in the body of the table is in G , so G is closed under \times_{20} .

G2 Associativity



Modular multiplication is associative.

G3 Identity

 We look for a row and column with the same label that repeat the table borders. 

The table shows that 1 is an identity element for \times_{20} on G .

G4 Inverses

 We check that each row contains the identity element 1, either on the main diagonal or symmetrically with respect to it. 

The table shows that 1 and 9 are self-inverse, and 3 and 7 are inverses of each other.

Since all four axioms hold, (G, \times_{20}) is a group.

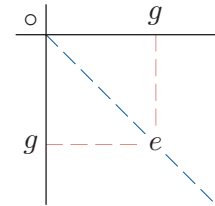


Figure 5 A self-inverse element g

Remember that a **self-inverse** element is one that is an inverse of itself. In a Cayley table each self-inverse element corresponds to an occurrence of the identity element e on the main diagonal, as shown in Figure 5.

Exercise E3

Let $G = \{\mathbf{I}, \mathbf{R}, \mathbf{S}, \mathbf{T}\}$ where

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{R} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{S} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Construct a Cayley table for the set G under matrix multiplication. Hence show that (G, \times) is a group. Determine whether it is an abelian group.

(Notice that \mathbf{I} , \mathbf{R} , \mathbf{S} and \mathbf{T} are all diagonal matrices and hence are straightforward to multiply together.)

In the next exercise you will need to construct Cayley tables using modular arithmetic. Remember that there are ways to make modular arithmetic calculations quicker and easier, as you saw in Subsection 3.3 of Unit A2 *Number systems*. For example, to work out $9 \times_{24} 15$, instead of starting by working out $9 \times 15 = 135$, you can proceed as follows:

$$\begin{aligned} 9 \times 15 &\equiv 9 \times 3 \times 5 \\ &\equiv 27 \times 5 \\ &\equiv 3 \times 5 \\ &\equiv 15 \pmod{24}. \end{aligned}$$

Thus $9 \times_{24} 15 = 15$.

Similarly, to work out $9 \times_{24} 21$, you can proceed as follows:

$$\begin{aligned} 9 \times 21 &\equiv 9 \times (-3) \\ &\equiv -27 \\ &\equiv -3 \\ &\equiv 21 \pmod{24}. \end{aligned}$$

Thus $9 \times_{24} 21 = 21$.

You can also make use of the fact that modular addition and modular multiplication are commutative binary operations, so a Cayley table for a set of numbers with one of these operations will be symmetric with respect to its main diagonal.

Exercise E4

In each of the following cases, construct a Cayley table for the set and binary operation, and hence determine whether they form a group.

- (a) $(\{0, 1, 2\}, +_3)$ (b) $(\{2, 4, 6\}, \times_8)$ (c) $(\{1, 5\}, \times_6)$
 (d) $(\{3, 9, 15, 21\}, \times_{24})$

Exercise E4(a) and (c) are particular examples of the first two of the following general results that you met in Unit B1 *Symmetry and groups*. (Here and elsewhere in this book, results from Book B are quoted with their original numbers.)

Standard finite groups of numbers

Theorem B8 For each integer $n \geq 2$, the set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ is a group under $+_n$.

Theorem B9 For each integer $n \geq 2$, the set U_n of all integers in \mathbb{Z}_n that are coprime to n is a group under \times_n .

Corollary B10 For each prime p , the set $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ is a group under \times_p . (Note that $U_p = \mathbb{Z}_p^*$ when p is prime.)

Exercise E5

List the elements of each of the following groups.

- (a) (U_{18}, \times_{18}) (b) (U_7, \times_7) (c) $(\mathbb{Z}_7^*, \times_7)$

In Unit B1 you met some useful facts that follow directly from the group axioms. Here is an important one to remember, from Subsection 4.1 of Unit B1.

In a group (G, \circ) we write composites of three or more elements such as $g \circ h \circ k$ and $g \circ h \circ k \circ l$ without brackets, because it follows from axiom G2 that any possible way of interpreting such a composite gives the same answer.

For example, the composite $g \circ h \circ k$ can be evaluated by interpreting it as either $g \circ (h \circ k)$ or $(g \circ h) \circ k$. It does not matter which of these expressions we choose, as they both give the same answer, by axiom G2.

Remember, though, that in general we cannot change the *order* of the elements in a composite of group elements. For example, $g \circ h \circ k$ is not necessarily equal to $h \circ g \circ k$. However, if the group is abelian, then we *can* change the order of the elements in a composite in any way we like, since all possible orders will give the same answer.

The two boxes below contain some other important results about groups that follow directly from the group axioms.

Uniqueness of the identity and of inverses

The following hold in any group.

Proposition B11 The identity element is unique. We usually denote it by e .

Proposition B12 Each element x has a unique inverse. We usually denote it by x^{-1} .

Basic properties of group elements

The following hold for any elements x, y, a and b of any group (G, \circ) .

Proposition B13 $(x^{-1})^{-1} = x$

Proposition B14 $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$

Proposition B15 **Left and Right Cancellation Laws**

If $x \circ a = x \circ b$, then $a = b$.

If $a \circ x = b \circ x$, then $a = b$.

You saw in Unit B1 that the Left and Right Cancellation Laws can be used to prove the following property of group tables.

Proposition B18

In a group table, each element of the group occurs exactly once in each row and exactly once in each column.

Thus, if you meet a Cayley table in which this property does not hold, then you can immediately conclude that it is not a group table. For example, if the set $\{e, a, b, c\}$ with binary operation \circ has the Cayley table

| \circ | e | a | b | c |
|---------|-----|-----|-----|-----|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | b | e |
| c | c | b | e | b |

then $(\{e, a, b, c\}, \circ)$ is not a group because b occurs more than once and a not at all in some rows and columns of the Cayley table.

It is important to remember that a group (G, \circ) consists of *two* things: the set G and the binary operation \circ . However, frequently for convenience we refer to a group (G, \circ) just as the group G , provided this will not cause confusion. For instance, we often do this in the following situations:

- where there is an ‘obvious’ binary operation under which a set G is a group
- where the binary operation associated with a set G is clear from the context
- where we are discussing a general, abstract group and do not need to refer to the binary operation.

For example, we might refer to the group (\mathbb{R}^*, \times) simply as ‘the group \mathbb{R}^* ’, since the only obvious binary operation under which \mathbb{R}^* is a group is multiplication.

1.2 Permutation groups

An important family of groups is that of groups of *permutations*.

A **permutation** of a finite set S is a one-to-one function from S to S . It can be written in **two-line form**. For example, the notation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 2 & 1 & 4 \end{pmatrix}$$

specifies that the permutation f maps 1 to 5, 2 to 6, 3 to 3, and so on.

A more convenient notation for permutations is **cycle form**. This notation depends on the fact that for any permutation f of a set S , if we write down all the elements of S and draw an arrow from each element to its image under f , then we obtain one or more **cycles**. For example, if we do this for the permutation f above, then we obtain the cycles shown in Figure 6.

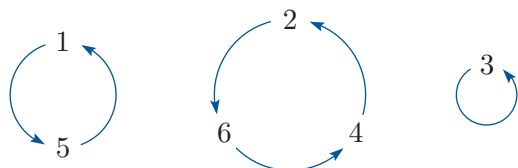


Figure 6 The cycles of the permutation f

Using these cycles, we write the permutation f above in cycle form as

$$f = (1\ 5)(2\ 6\ 4)(3).$$

In the cycle form of a permutation, each cycle can be written with any of its symbols as the first symbol, and the cycles can be written in any order. For example, an alternative way to write the permutation f above is

$$f = (3)(6\ 4\ 2)(5\ 1).$$

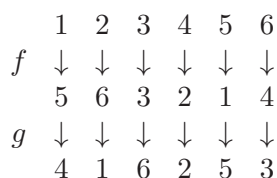
However, if the symbols in the permutation are numbers then we usually write the smallest symbol in each cycle first and arrange the cycles with their smallest symbols in increasing order, unless there is a reason to do otherwise.

The **length** of a cycle is the number of symbols in it, and a cycle of length r is called an **r -cycle**. We usually omit 1-cycles from the cycle form of a permutation. So our standard way to write the permutation f above is

$$f = (1\ 5)(2\ 6\ 4).$$

Note that the cycles in the cycle form of a permutation are **disjoint** – that is, they have no elements in common.

Any two permutations of the same set S can be composed to give another permutation of S . For example, if f is the permutation $(1\ 5)(2\ 6\ 4)$ above and g is the permutation $(1\ 5\ 4\ 3\ 6)$, then the composite $g \circ f$ (that is, f followed by g) can be illustrated as follows.



This diagram shows, for example, that f maps 1 to 5 and then g maps 5 to 4, so altogether $g \circ f$ maps 1 to 4.



The worked exercise below demonstrates how to compose two permutations by directly using their cycle forms, for the same two permutations f and g as above.

Worked Exercise E3



Find, in cycle form, the composite permutation $g \circ f$ of the permutations

$$f = (1\ 5)(2\ 6\ 4) \quad \text{and} \quad g = (1\ 5\ 4\ 3\ 6).$$



Solution

 We start a cycle of $g \circ f$ with the smallest symbol, 1. The permutation f maps 1 to 5 and then g maps 5 to 4, so $g \circ f$ maps 1 to 4. 



$$g \circ f = (1\ 5\ 4\ 3\ 6) \circ (1\ 5)(2\ 6\ 4) = (1\ 4\ \dots$$

 To continue the cycle, we find the image of 4. The permutation f maps 4 to 2 and g fixes 2, so $g \circ f$ maps 4 to 2. 

$$= (1\ 4\ 2\ \dots$$

 Continuing in this way, we find that $g \circ f$ maps 2 to 1, completing the cycle. 

$$= (1\ 4\ 2)\dots$$

 We start the next cycle with the smallest symbol whose image under $g \circ f$ we have not yet found, and continue in a similar way until we have included all the symbols. 

$$g \circ f = (1\ 5\ 4\ 3\ 6) \circ (1\ 5)(2\ 6\ 4) = (1\ 4\ 2)(3\ 6)(5) = (1\ 4\ 2)(3\ 6)$$

Remember that the order in which you compose permutations is important: if f and g are permutations, then the composite $f \circ g$ may not be equal to the composite $g \circ f$.

Exercise E6

Determine the cycle form of each of the following composites of permutations.

$$(a) \ (1\ 2\ 7\ 5)(3\ 8\ 4) \circ (1\ 3\ 6\ 7\ 5) \quad (b) \ (1\ 3\ 7)(2\ 5\ 4) \circ (2\ 4)(3\ 8)(5\ 6)$$

You can use the method demonstrated in Worked Exercise E3 to compose any number of permutations. For example, in Exercise E7 (below) the first (right-most) permutation maps 1 to 7, then the next permutation maps 7 to 4, and finally the third permutation maps 4 to 5, so altogether 1 is mapped to 5.

Exercise E7

Determine the cycle form of the following composite of permutations.

$$(1\ 4\ 5\ 6) \circ (2\ 3\ 7\ 4\ 8) \circ (1\ 7\ 6)(3\ 2\ 5).$$

Any permutation is equal to the composite (in any order) of its disjoint cycles. For example,

$$(1\ 5)(2\ 6\ 4) = (1\ 5) \circ (2\ 6\ 4) = (2\ 6\ 4) \circ (1\ 5).$$

However, not every composite of cycles can be interpreted as the cycle form of a permutation. For example, $(1\ 2) \circ (2\ 3)$ is a composite of cycles, but $(1\ 2)(2\ 3)$ is not the cycle form of a permutation because the two cycles here are *not disjoint* (they have the symbol 2 in common).

The inverse of a permutation of a set S is another permutation of S . For example, if $f = (1\ 5)(2\ 6\ 4)$, as above, then the effect of f is

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ f & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 6 & 3 & 2 & 1 & 4 \end{array},$$

so the effect of its inverse f^{-1} , obtained by reversing the arrows, is

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ f^{-1} & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ & 5 & 6 & 3 & 2 & 1 & 4 \end{array}.$$

The next worked exercise demonstrates how to find the inverse of a permutation directly from its cycle form.

Worked Exercise E4

Find, in cycle form, the inverse of the permutation $f = (1\ 5)(2\ 6\ 4)$.

Solution

 We simply reverse all the cycles. 

$$f^{-1} = (5\ 1)(4\ 6\ 2)$$

 We then write f^{-1} in the usual form, with the smallest symbol in each cycle first. 

$$= (1\ 5)(2\ 4\ 6)$$

Exercise E8

Find the inverse of each of the following permutations.

(a) $(1\ 7\ 5\ 2)(3\ 8\ 4)$ (b) $(1\ 4)(2\ 3)(6\ 8)$

The technique of reversing the cycles to find the inverse of a permutation works *only if the permutation is in cycle form*. For example, the inverse of the composite permutation $(1\ 2\ 3) \circ (3\ 4)$ is *not* obtained by reversing the cycles $(1\ 2\ 3)$ and $(3\ 4)$, because these cycles are not disjoint.

A 2-cycle is called a **transposition**. Any cycle can be expressed as a composite of transpositions, as follows.

Strategy B10

To express a cycle $(a_1\ a_2\ a_3\ \dots\ a_r)$ as a composite of transpositions, write the transpositions

$$(a_1\ a_2), (a_1\ a_3), (a_1\ a_4), \dots, (a_1\ a_r)$$

in reverse order and form their composite. That is,

$$(a_1\ a_2\ a_3\ \dots\ a_r) = (a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \dots \circ (a_1\ a_3) \circ (a_1\ a_2).$$

For example, as you can check by composing the transpositions,



$$(1\ 2\ 3\ 4\ 5\ 6) = (1\ 6) \circ (1\ 5) \circ (1\ 4) \circ (1\ 3) \circ (1\ 2).$$

Because any cycle can be expressed as a composite of transpositions, so can any permutation, as illustrated in the next worked exercise.

Worked Exercise E5

Write the permutation $(1\ 5\ 7\ 2)(3\ 4\ 6)$ as a composite of transpositions.

Solution

 Use Strategy B10 to write each cycle in the permutation as a composite of transpositions. 

$$(1\ 5\ 7\ 2)(3\ 4\ 6) = (1\ 2) \circ (1\ 7) \circ (1\ 5) \circ (3\ 6) \circ (3\ 4)$$

Exercise E9

Write the permutation $(1\ 5\ 3)(2\ 4\ 7\ 9\ 6)$ as a composite of transpositions.

There are many different ways to express a particular permutation as a composite of transpositions. For example, by Strategy B10 the permutation $(3\ 4\ 5)$ can be written as

$$(3\ 5) \circ (3\ 4),$$

but since $(3\ 4\ 5) = (4\ 5\ 3)$, it can also be written as

$$(4\ 3) \circ (4\ 5).$$

A third way to write it is

$$(3\ 5) \circ (3\ 4) \circ (1\ 2) \circ (1\ 2),$$

since $(1\ 2)$ is the inverse of itself.

However, we have the following theorem.

Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

We say that a permutation is **even** if it can be expressed as a composite of an even number of transpositions, and **odd** if it can be expressed as a composite of an odd number of transpositions. The evenness or oddness of a permutation is called its **parity**.

The parity of a permutation has the properties in the box below.

The first two properties come from the fact that an r -cycle can be expressed as a composite of $r - 1$ transpositions, by Strategy B10. The third and fourth properties come from considering the numbers of transpositions in composites of permutations.

Properties of the parity of a permutation

- A cycle of odd length is an even permutation.
- A cycle of even length is an odd permutation.
- The composite of two odd or two even permutations is even.
- The composite of an even and an odd permutation is odd.

We can use these four properties to determine the parity of any permutation expressed in cycle form, as demonstrated in the following worked exercise.

Worked Exercise E6

Determine the parity of the permutation

$$f = (1\ 3\ 4)(2\ 6)(5\ 9\ 7\ 8).$$

Solution

The cycles $(1\ 3\ 4)$, $(2\ 6)$ and $(5\ 9\ 7\ 8)$ are even, odd and odd, respectively. Hence the permutation f is

$$\text{even} + \text{odd} + \text{odd} = \text{even}.$$

Exercise E10

Determine the parity of each of the following permutations.

$$(a) \ (1\ 5\ 8)(2\ 7\ 3\ 4) \quad (b) \ (1\ 8)(2\ 7)(3\ 5\ 4\ 6)$$

The method of determining parity demonstrated in Worked Exercise E6 shows us that any two permutations with the same **cycle structure** (that is, the same number of cycles of each length) have the same parity. For example, the permutations $(1\ 2)(3\ 4\ 6)$ and $(1\ 4\ 3)(2\ 5)$ have the same cycle structure and hence the same parity.

In Unit B3 *Permutations* you saw proofs of the following facts.

The symmetric group S_n and the alternating group A_n

Theorems B52 and B53 For each positive integer n , the set S_n of all permutations of the set $\{1, 2, \dots, n\}$ is a group under function composition, called the **symmetric group of degree n** . It has order $n!$.

Theorems B61 and B62 For each positive integer n , the set A_n of all even permutations of the set $\{1, 2, \dots, n\}$ is a group under function composition, called the **alternating group of degree n** . For $n \geq 2$ it has order $\frac{1}{2}n!$.

The identity element of both the group S_n and the group A_n is the permutation that maps every element of the set $\{1, 2, \dots, n\}$ to itself, which we call the **identity permutation** and usually denote by e . The group S_n is non-abelian for $n \geq 3$ and the group A_n is non-abelian for $n \geq 4$.

The group A_n is a *subgroup* of the group S_n : you will revise the idea of a subgroup in Subsection 1.4.

A group whose elements are permutations of a finite set and whose binary operation is function composition is called a **permutation group**.

1.3 Symmetry groups

A rich source of examples of groups, many of them non-abelian, is the symmetry of figures. A **figure** in \mathbb{R}^2 is any subset of \mathbb{R}^2 , such as a triangle, a square, a rectangle or a line. Similarly, a **figure** in \mathbb{R}^3 is any subset of \mathbb{R}^3 , such as a tetrahedron or a cuboid. Some examples of figures are shown in Figure 7. A figure in \mathbb{R}^2 is called a **plane figure**. A figure in \mathbb{R}^3 is called a **solid figure** if it has non-zero height, non-zero width and non-zero depth.



Figure 7 Examples of plane and solid figures

An **isometry** of \mathbb{R}^2 is a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ that preserves distances; that is, for all points $X, Y \in \mathbb{R}^2$, the distance between $f(X)$ and $f(Y)$ is the same as the distance between X and Y . A **symmetry** of a plane figure is an isometry of \mathbb{R}^2 that maps the figure to itself. An isometry of \mathbb{R}^3 , and a symmetry of a 3-dimensional figure, are defined in an analogous way.

It is straightforward to check that the set of symmetries of a figure, with the binary operation of function composition, satisfies the group axioms: try thinking this through for yourself. So we have the following theorem.

Theorem B21

If F is a figure (in \mathbb{R}^2 or \mathbb{R}^3), then the set $S(F)$ of all symmetries of F is a group under function composition, called the **symmetry group** of F .

For example, you have met $S(\triangle)$, $S(\square)$, $S(\square)$ and $S(\diamond)$, the symmetry groups of the equilateral triangle, the square, the rectangle and the regular hexagon, with orders 6, 8, 4 and 12, respectively. You have also met $S(\text{tet})$ and $S(\text{cuboid})$, the symmetry groups of the regular tetrahedron and a cuboid with no square faces, with orders 24 and 8, respectively.

The identity element of the symmetry group of a figure F is called the **identity symmetry** of F , and is usually denoted by e .

The groups $S(\triangle)$, $S(\square)$ and $S(\square)$ are summarised below. Figures 8, 9 and 10 show the elements of these groups, except the identity symmetry, and Tables 1, 2 and 3 describe these elements. Each element can be represented as a permutation of the labels of the vertex locations, as given in the tables. For example, the symmetry a of the equilateral triangle is represented by the permutation $(1\ 2\ 3)$ because it maps the vertex at location 1 to the vertex at location 2, the vertex at location 2 to the vertex at location 3, and the vertex at location 3 to the vertex at location 1. Remember that the numbers label the vertex *locations* rather than the vertices themselves: the labels do not move when the figure is transformed by a symmetry.

Here and throughout the group theory units we express angles of rotation of plane figures in radians *anticlockwise*, unless otherwise stated.

Table 1 The elements of $S(\triangle)$

| Symmetry | Description | Representation |
|----------|-------------------------------------|----------------|
| e | identity | e |
| a | rotation through $2\pi/3$ | $(1\ 2\ 3)$ |
| b | rotation through $4\pi/3$ | $(1\ 3\ 2)$ |
| r | reflection in axis through vertex 1 | $(2\ 3)$ |
| s | reflection in axis through vertex 2 | $(1\ 3)$ |
| t | reflection in axis through vertex 3 | $(1\ 2)$ |

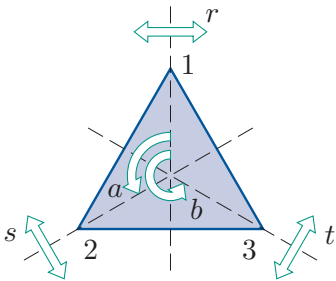


Figure 8 $S(\triangle)$

Table 2 The elements of $S(\square)$

| Symmetry | Description | Representation |
|----------|---|----------------|
| e | identity | e |
| a | rotation through $\pi/2$ | $(1\ 2\ 3\ 4)$ |
| b | rotation through π | $(1\ 3)(2\ 4)$ |
| c | rotation through $3\pi/2$ | $(1\ 4\ 3\ 2)$ |
| r | reflection in vertical axis | $(1\ 4)(2\ 3)$ |
| s | reflection in diagonal through vertex 1 | $(2\ 4)$ |
| t | reflection in horizontal axis | $(1\ 2)(3\ 4)$ |
| u | reflection in diagonal through vertex 2 | $(1\ 3)$ |

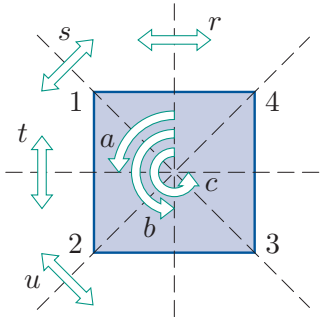


Figure 9 $S(\square)$

Table 3 The elements of $S(\square)$

| Symmetry | Description | Representation |
|----------|-------------------------------|----------------|
| e | identity | e |
| a | rotation through π | $(1\ 3)(2\ 4)$ |
| r | reflection in vertical axis | $(1\ 4)(2\ 3)$ |
| s | reflection in horizontal axis | $(1\ 2)(3\ 4)$ |

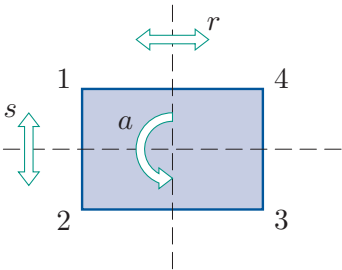


Figure 10 $S(\square)$

We can compose the symmetries of a figure by composing the permutations that represent them. For example, for the symmetries s and b in $S(\triangle)$ we have

$$b \circ s = (1\ 3\ 2) \circ (1\ 3) = (1\ 2)(3) = (1\ 2) = t.$$

By combining all pairs of symmetries in each of $S(\triangle)$, $S(\square)$ and $S(\square)$ in this way, we obtain the following group tables.

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

$S(\triangle)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

$S(\square)$

| \circ | e | a | r | s |
|---------|-----|-----|-----|-----|
| e | e | a | r | s |
| a | a | e | s | r |
| r | r | s | e | a |
| s | s | r | a | e |

$S(\square)$

Exercise E11

Use the group table for $S(\triangle)$ to determine the following.

- (a) $a \circ s$ (b) b^{-1} (c) $b \circ r \circ a$

Hint: In part (c), write $b \circ r \circ a$ as either $b \circ (r \circ a)$ or $(b \circ r) \circ a$.

A symmetry of a plane figure is **direct** if its effect can be demonstrated using a model of the figure without removing the model from the plane. For a solid figure, a symmetry is **direct** if its effect can be demonstrated directly in space using a model of the figure. The symmetries of a plane or solid figure that are not direct are called **indirect**.

If a plane figure is bounded, then its direct symmetries are rotations about a central point (including the identity symmetry, which is a rotation through 0 radians), and its indirect symmetries, if it has any, are reflections in lines through this point. For example, in $S(\triangle)$, the direct symmetries are e , a and b , and the indirect symmetries are r , s and t .

If a solid figure is bounded, then its direct symmetries are rotations about lines, and its indirect symmetries, if it has any, include reflections in planes and possibly other types of indirect symmetries.

Properties of direct and indirect symmetries

- The composite of two direct symmetries or two indirect symmetries is direct.
- The composite of a direct symmetry and an indirect symmetry is indirect.

Theorem B22 If a figure has a finite number of symmetries, then either they are all direct or half are direct and half are indirect.

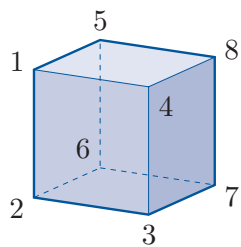


Figure 11 The cube

The symmetries of a solid figure can be represented by permutations of its vertex location labels in the same way as those of a plane figure. For example, if the vertex locations of the cube are labelled as shown in Figure 11, then the reflection in the horizontal plane through the centre of the cube is represented by the permutation $(1\ 2)(3\ 4)(5\ 6)(7\ 8)$.

For brevity, from now on in this book we will use phrases such as ‘vertex labels’, rather than the more correct ‘labels of the vertex locations’, and ‘the line 14’, rather than the more correct ‘the line through the vertices at locations 1 and 4’.

Exercise E12

This question is about the labelled cube in Figure 11.

- Describe geometrically the symmetry of the cube represented by each of the following permutations.
 - $(1\ 8)(2\ 7)$
 - $(1\ 4\ 8\ 5)(2\ 3\ 7\ 6)$
- Compose the two permutations in part (a) in each of the two possible orders, and describe geometrically the symmetry represented by each of the resulting two composite symmetries.
- Write down, in cycle form, the permutation that represents each of the following symmetries of the cube.
 - Rotation through π about the line that passes through the midpoints of the faces 1265 and 4378.
 - The two non-trivial rotations about the line that passes through the vertices 1 and 7.

1.4 Subgroups

We make the following definition.

Definition

A **subgroup** of a group (G, \circ) is a group (H, \circ) , where H is a subset of G .

Notice that for a group H to be a subgroup of a group G the binary operation must be the *same* for G and H .

For example, the group $(\mathbb{Q}, +)$ is a subgroup of the group $(\mathbb{R}, +)$, since \mathbb{Q} is a subset of \mathbb{R} and the two groups have the same binary operation. On the other hand, the group (\mathbb{R}^*, \times) is not a subgroup of the group $(\mathbb{R}, +)$, even though \mathbb{R}^* is a subset of \mathbb{R} , because the two groups do not have the same binary operation.

Every group of order greater than 1 has at least two subgroups, namely the group itself and the **trivial subgroup**, whose only element is the identity element.

The following two theorems were proved in Unit B2 *Subgroups and isomorphisms*.

Theorem B23 Identity and inverses in a subgroup

Let (G, \circ) be a group with a subgroup (H, \circ) .

- (a) The identity element of (H, \circ) is the same as the identity element of (G, \circ) .
- (b) For each element h of H , the inverse of h in (H, \circ) is the same as its inverse in (G, \circ) .

Theorem B24 Subgroup test

Let (G, \circ) be a group with identity element e , and let H be a subset of G . Then (H, \circ) is a subgroup of (G, \circ) if and only if the following three properties hold.

SG1 Closure For all x, y in H , the composite $x \circ y$ is in H .

SG2 Identity The identity element e of G is in H .

SG3 Inverses For each x in H , its inverse x^{-1} in G is in H .

We refer to properties SG1, SG2 and SG3 as the three **subgroup properties**. Subgroup property SG1 (closure) is the same as group axiom G1 (closure). However, subgroup properties SG2 (identity) and SG3 (inverses) are not the same as group axioms G3 (identity) and G4 (inverses): these two subgroup properties are concerned with *belonging to*, whereas the corresponding two group axioms are concerned with *existence*.

Notice that before you check the three subgroup properties for a subset H of a group G , you first have to be sure that H is a *subset* of G , and that the binary operation \circ defined on H is the same as that defined on G . If either of these conditions do not hold, then (H, \circ) cannot be a subgroup of (G, \circ) .

For a *finite* subset of a group, if you suspect that the subset *is* a subgroup, then it can be helpful to construct a Cayley table for the subset before you try to apply Theorem B24. In the next exercise you can practise applying Theorem B24 to finite subsets of a group.

Exercise E13

Determine whether each of the following sets, with the binary operation \times_{25} , is a subgroup of the group (U_{25}, \times_{25}) .

(Remember that U_{25} is the set of integers in \mathbb{Z}_{25} coprime to 25.)

- (a) $A = \{1, 5, 10, 15, 20\}$ (b) $B = \{1, 6, 11, 16, 21\}$
(c) $C = \{1, 9, 11, 21\}$

As with groups in general, we often refer to a subgroup (H, \circ) of a group (G, \circ) simply as the subgroup H if the binary operation is clear from the context. This is done in the solution to Exercise E13. Also, if you are asked to show that a particular subset H of a group G is a subgroup of G , then you should assume that the binary operation on H is the same as on G .

Exercise E14

Let x be a self-inverse element of a group (G, \circ) with identity e . Show that $\{e, x\}$ is a subgroup of G .

You will have an opportunity to practise applying Theorem B24 to infinite subsets of infinite groups in the next section. In the rest of this subsection we will look briefly at some subsets of particular types of finite groups, namely symmetry groups and symmetric groups. We will also revise Lagrange's Theorem, which is about subgroups of finite groups.

Subgroups of symmetry groups

In Unit B2 you met the following result.

Theorem B25

Let F be a figure in \mathbb{R}^2 or \mathbb{R}^3 . Then the set of direct symmetries of F , denoted by $S^+(F)$, is a subgroup of the symmetry group $S(F)$ of F .

For example, the set $S^+(\triangle) = \{e, a, b\}$ of direct symmetries of the equilateral triangle is a subgroup of $S(\triangle)$. (The non-identity elements of $S(\triangle)$ are shown in Figure 12.)

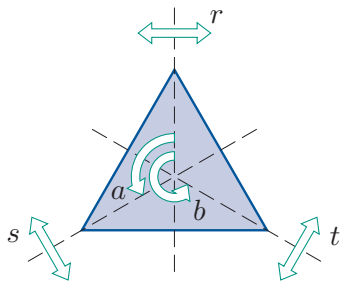


Figure 12 $S(\triangle)$

You also saw that you can find subgroups of a symmetry group $S(F)$ by modifying the figure F . For example, the plane figure in Figure 13 is a modified version of the equilateral triangle in Figure 12. The only symmetries of the original triangle that are also symmetries of the modified triangle are e and r , so $\{e, r\}$ is a subgroup of $S(\triangle)$.

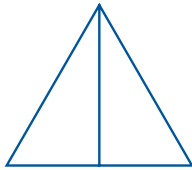


Figure 13 A modified equilateral triangle

Table 4 lists all the subgroups of the group $S(\triangle)$: there are six altogether. The three subgroups of order 2 can be obtained by modifying the triangle in ways similar to that shown in Figure 13. Alternatively, we can use the fact that if x is any self-inverse element in a group G with identity e , then $\{e, x\}$ is a subgroup of G , as shown in the solution to Exercise E14. The three elements r , s and t of $S(\triangle)$ are all self-inverse.

Table 4 The subgroups of $S(\triangle)$

| Order | Number of subgroups | Subgroups |
|-------|---------------------|--------------------------------|
| 1 | 1 | $\{e\}$ |
| 2 | 3 | $\{e, r\}, \{e, s\}, \{e, t\}$ |
| 3 | 1 | $\{e, a, b\}$ |
| 6 | 1 | $S(\triangle)$ |

Exercise E15

The non-identity elements of the symmetry group $S(\square)$ are shown in Figure 14. The group $S(\square)$ has ten subgroups:

- (a) one subgroup of order 1
- (b) five subgroups of order 2
- (c) three subgroups of order 4
- (d) one subgroup of order 8.

Write down as many of these subgroups as you can. (Do not look back to where these subgroups are given in Book B!)

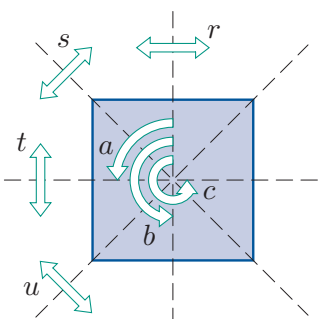


Figure 14 $S(\square)$

Subgroups of symmetric groups

In Unit B3 you met various subgroups of symmetric groups. Each symmetric group S_n has the alternating group A_n as a subgroup, as mentioned in Subsection 1.3.

One way to find another subgroup of a symmetric group S_n is to draw a suitable figure, label its vertices (or some other suitable features, such as its edges) with some or all of the symbols from the set $\{1, 2, \dots, n\}$, and represent the symmetries of the figure as permutations of these labels. For example, the labelled rectangle in Figure 15 gives the following subgroup of S_6 :

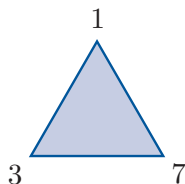
$$\{e, (1\ 3)(4\ 6), (1\ 6)(3\ 4), (1\ 4)(3\ 6)\}.$$



Figure 15 A labelled rectangle

Exercise E16

Use the labelled figure below to find a subgroup of the symmetric group S_7 .



Another way to find a subgroup of a symmetric group S_n is to find all the permutations in S_n that fix a particular symbol from the set $\{1, 2, \dots, n\}$, or that fix each symbol in some set of symbols. For example, $\{e, (1\ 4)\}$ is the subgroup of S_4 whose elements are the permutations in S_4 that fix the symbols in the set $\{2, 3\}$.

There are many more ways to find a subgroup of a symmetric group. Another way is given in the next exercise.

Exercise E17

- Let n be a positive integer and let A be any subset of the set $S = \{1, 2, \dots, n\}$. Let G be the subset of the symmetric group S_n that consists of all the permutations in S_n that map each element of A to another element of A . By using Theorem B24 (Subgroup test), prove that G is a subgroup of S_n .
- List the elements of the group G defined in part (a) when $n = 5$ and $A = \{4, 5\}$.

Lagrange's Theorem

The following fundamental theorem was proved in Unit B4 *Lagrange's Theorem and small groups*.

Theorem B68 Lagrange's Theorem

Let G be a finite group and let H be any subgroup of G . Then the order of H divides the order of G .

The converse of Lagrange's Theorem is *not* true. In other words, if m is a positive divisor of the order of a group G , then there is no guarantee that G has a subgroup of order m . It may have such a subgroup, or it may not.

2 Matrix groups

Unlike Sections 1 and 3, this section does not contain revision of group theory that you have already met in Book B. It is about a new topic: matrix groups.

In Subsections 3.1 and 4.1 of Unit C1 *Linear equations and matrices* you saw that, for any positive integers m and n ,

- the set of all $m \times n$ matrices with real entries forms a group under matrix addition, denoted by $M_{m,n}$
- the set of all *invertible* $n \times n$ matrices with real entries forms a group under matrix multiplication.

The second of these groups is called the **general linear group of degree n** (over the real numbers), and is denoted by $GL(n)$. This name is used because the word 'linear' is associated with matrix algebra – known as *linear algebra* (it arises from systems of linear equations) – and the word 'general' distinguishes this group from the *special linear group of degree n* , which is defined later in this section.

Throughout this book we will work frequently with $GL(2)$, the group of invertible 2×2 matrices with real entries under matrix multiplication, and with some of its subgroups. This section introduces you to some of these subgroups. We will assume throughout that by 'matrix' we mean a matrix with entries that are real numbers (rather than complex numbers, for example).

First, here is a reminder of some important properties of 2×2 matrices that we will need. You met these properties in Unit C1. Most of them generalise to properties of $n \times n$ matrices, but in Book E we will need them only for 2×2 matrices.

In the box below, and generally throughout this book, we write a product of two matrices in the form \mathbf{AB} , in the usual way, rather than making the binary operation explicit by writing $\mathbf{A} \times \mathbf{B}$.

Properties of 2×2 matrices

1. The 2×2 **identity matrix**

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

has the property that

$$\mathbf{AI} = \mathbf{A} = \mathbf{IA}$$

for each 2×2 matrix \mathbf{A} .

2. If \mathbf{A} is a 2×2 matrix, then there *may* exist a 2×2 matrix, denoted by \mathbf{A}^{-1} , such that

$$\mathbf{AA}^{-1} = \mathbf{I} = \mathbf{A}^{-1}\mathbf{A}.$$

If such a matrix \mathbf{A}^{-1} exists, then it is unique and is called the **inverse** of \mathbf{A} , and we say that \mathbf{A} is **invertible**.

3. The **determinant** of $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by

$$\det \mathbf{A} = ad - bc.$$

A 2×2 matrix \mathbf{A} is invertible if and only if $\det \mathbf{A} \neq 0$.

4. If $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, then

$$\mathbf{A}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

5. For all 2×2 matrices \mathbf{A} and \mathbf{B} ,

$$\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B}).$$

6. For all invertible 2×2 matrices \mathbf{A} and \mathbf{B} ,

$$(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1},$$

$$(\mathbf{A}^{-1})^{-1} = \mathbf{A},$$

$$\det \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}.$$

Exercise E18

Determine whether each of the following matrices is invertible, and write down its inverse if it exists.

(a) $\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 2 & -2 \\ 1 & -1 \end{pmatrix}$

Although you have already seen in Subsection 4.1 of Unit C1 that the set of invertible 2×2 matrices is a group under matrix multiplication, a proof of this fact is given below, to help familiarise you with this group. The proof given here is only for 2×2 matrices, rather than more generally for $n \times n$ matrices, as this is all we need here.

Theorem E1

The set of invertible 2×2 matrices is a group under matrix multiplication.

Proof Let G be the set of invertible 2×2 matrices. We show that the four group axioms hold for G under matrix multiplication.

G1 Closure

Let \mathbf{A} and \mathbf{B} be any elements of G . Then \mathbf{AB} is a 2×2 matrix. Also, since \mathbf{A} and \mathbf{B} are invertible, $\det \mathbf{A} \neq 0$ and $\det \mathbf{B} \neq 0$, so

$$\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B}) \neq 0.$$

Hence \mathbf{AB} is invertible. Therefore $\mathbf{AB} \in G$. So G is closed under matrix multiplication.

G2 Associativity

Matrix multiplication is associative.

G3 Identity

The 2×2 identity matrix \mathbf{I} is an invertible 2×2 matrix, so $\mathbf{I} \in G$ and we have

$$\mathbf{AI} = \mathbf{A} = \mathbf{IA}$$

for each $\mathbf{A} \in G$. Thus \mathbf{I} is an identity element in G .

G4 Inverses

Let \mathbf{A} be any element of G . Then \mathbf{A} is invertible, so its inverse \mathbf{A}^{-1} exists and is itself an invertible 2×2 matrix (with inverse \mathbf{A}). Hence $\mathbf{A}^{-1} \in G$ and we have

$$\mathbf{AA}^{-1} = \mathbf{I} = \mathbf{A}^{-1}\mathbf{A}.$$

Thus each element $\mathbf{A} \in G$ has an inverse element $\mathbf{A}^{-1} \in G$.

Hence (G, \times) satisfies the four group axioms and so is a group. ■

As mentioned earlier, the group in Theorem E1 is called the **general linear group of degree 2** and is denoted by $\text{GL}(2)$.

Now let us look at some subgroups of $GL(2)$. The first worked exercise in this subsection shows that the set of all *lower triangular* matrices in $GL(2)$ is a subgroup of $GL(2)$. Recall that a **lower triangular** matrix is a matrix each of whose entries above the main diagonal is zero. So a 2×2 lower triangular matrix is a matrix of the form

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix},$$

where $a, c, d \in \mathbb{R}$.

Worked Exercise E7



Show that the set L of lower triangular matrices in $GL(2)$ is a subgroup of $GL(2)$.

Solution

We show that the three subgroup properties hold for L .

SG1 Closure

Let $\mathbf{A}, \mathbf{B} \in L$.

 We need to show that $\mathbf{AB} \in L$. We know that $\mathbf{AB} \in GL(2)$ since $\mathbf{A}, \mathbf{B} \in GL(2)$ and $GL(2)$ is a group, so all we need to show is that \mathbf{AB} is lower triangular. 

Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$. Hence

$$\mathbf{AB} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} = \begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix}.$$

This is a lower triangular matrix, so $\mathbf{AB} \in L$.

Thus L is closed under matrix multiplication.



SG2 Identity

The identity element $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of $GL(2)$ is lower triangular.

Hence $\mathbf{I} \in L$.

SG3 Inverses

Let $\mathbf{A} \in L$.

 We need to show that $\mathbf{A}^{-1} \in L$. We know that $\mathbf{A}^{-1} \in GL(2)$ since $\mathbf{A} \in GL(2)$ and $GL(2)$ is a group, so all we need to show is that \mathbf{A}^{-1} is lower triangular. 

Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix},$$

for some $r, t, u \in \mathbb{R}$.

The inverse of \mathbf{A} in $\text{GL}(2)$ is

$$\mathbf{A}^{-1} = \frac{1}{ru} \begin{pmatrix} u & 0 \\ -t & r \end{pmatrix} = \begin{pmatrix} 1/r & 0 \\ -t/ru & 1/u \end{pmatrix}.$$

This is a lower triangular matrix, so $\mathbf{A}^{-1} \in L$. Thus L contains the inverse of each of its elements.

Since the three subgroup properties hold, L is a subgroup of $\text{GL}(2)$.

The set L in Worked Exercise E7, that is, the set of lower triangular matrices in $\text{GL}(2)$, can be described without reference to $\text{GL}(2)$ as the set of invertible 2×2 lower triangular matrices. We can specify it algebraically by using the fact that the 2×2 lower triangular matrix

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

is invertible if and only if its determinant

$$ad - 0 \times c = ad$$

is non-zero. This gives

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0 \right\}.$$

It can be shown in a similar way to the solution to Worked Exercise E7 that the set U of all *upper triangular* matrices in $\text{GL}(2)$ is a subgroup of $\text{GL}(2)$. Remember that an **upper triangular** matrix is a matrix each of whose entries below the main diagonal is zero. The group U can be specified in a similar way to the group L as follows:

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\}.$$

The next exercise is about the set D of all *diagonal* matrices in $\text{GL}(2)$. Remember that a **diagonal** matrix is a matrix each of whose entries not on the main diagonal is 0. So a 2×2 diagonal matrix is a matrix of the form

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},$$

where $a, d \in \mathbb{R}$.

Exercise E19

Show that the set D of diagonal matrices in $\text{GL}(2)$ is a subgroup of $\text{GL}(2)$.

The next exercise introduces another subgroup of $\text{GL}(2)$.

Exercise E20

Show that the set H of matrices in $\text{GL}(2)$ with determinant 1 is a subgroup of $\text{GL}(2)$.

The group in Exercise E20 is called the **special linear group of degree 2** and is denoted by $\text{SL}(2)$. (The proof in the solution to Exercise E20 can be generalised to show that for any positive integer n the set of matrices in $\text{GL}(n)$ with determinant 1 is a subgroup of $\text{GL}(n)$; this group is known as the *special linear group of degree n* (over the real numbers) and is denoted by $\text{SL}(n)$.)

The general linear group $\text{GL}(2)$ and the four subgroups of $\text{GL}(2)$ that you have met so far will be used frequently later in this book, and are summarised in the box below.

Some standard matrix groups

The group $\text{GL}(2)$, the group of all invertible 2×2 matrices under matrix multiplication, is given by

$$\text{GL}(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}.$$

Its subgroups include the following.

- The group $\text{SL}(2)$ of all 2×2 matrices with determinant 1:

$$\text{SL}(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}.$$

- The group L of all invertible 2×2 lower triangular matrices:

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0 \right\}.$$

- The group U of all invertible 2×2 upper triangular matrices:

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\}.$$

- The group D of all invertible 2×2 diagonal matrices:

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\}.$$

The group $\text{GL}(2)$ has very many more subgroups than the four above.

The next worked exercise concerns a subgroup of $\text{GL}(2)$ whose description is a little more complicated than those that you have met so far.

Worked Exercise E8

Show that the set

$$Y = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$$

is a group under matrix multiplication.

Solution



The set Y is a *subset* of the group $\text{GL}(2)$, because each matrix

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

in Y has determinant

$$1 \times 1 - b \times 0 = 1$$

and is therefore invertible. Also, the binary operation specified for Y is the same as the binary operation of $\text{GL}(2)$.

 Therefore, to show that Y is a group, we can show that it is a subgroup of $\text{GL}(2)$: we do not need to check the four group axioms from scratch. 

We show that the three subgroup properties hold for Y .


SG1 Closure

Let $\mathbf{A}, \mathbf{B} \in Y$. Then


$$\mathbf{A} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

for some $m, n \in \mathbb{Z}$. So

$$\mathbf{AB} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix}.$$

 To check that $\mathbf{AB} \in Y$, we have to check that it is of the form specified before the colon in the definition of Y , namely

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

and also that it satisfies the condition given after the colon, namely $b \in \mathbb{Z}$. 

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = m + n$. Also $m + n$ is an integer since both m and n are integers. So $\mathbf{AB} \in Y$. Thus Y is closed under matrix multiplication.

SG2 Identity

The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of $\text{GL}(2)$ is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = 0$. Thus $\mathbf{I} \in Y$.

SG3 Inverses

Let $\mathbf{A} \in Y$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

for some $n \in \mathbb{Z}$. The inverse of \mathbf{A} in $\text{GL}(2)$ is

$$\mathbf{A}^{-1} = \frac{1}{1} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = -n$. Also, $-n$ is an integer since n is an integer. So $\mathbf{A}^{-1} \in Y$. Thus Y contains the inverse of each of its elements.

Since the three subgroup properties hold, Y is a subgroup of $\text{GL}(2)$. Hence it is a group under matrix multiplication.

Notice that when subgroup property SG1 was checked in Worked Exercise E8, the two general elements \mathbf{A} and \mathbf{B} of the set

$$Y = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$$

were taken to be

$$\mathbf{A} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

So two new symbols, m and n , were chosen to represent the two variables needed; the symbol b from the definition of the set Y was not used at all. It is sometimes convenient to choose completely new symbols in this way, to prevent possible confusion when we later compare an element that we have found (such as a product matrix \mathbf{AB} or an inverse matrix \mathbf{A}^{-1}) to the general form of an element of a set. An alternative to choosing completely new symbols is to use subscripts: for example, here we could take

$$\mathbf{A} = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}.$$

The next worked exercise involves a subset of $\text{GL}(2)$ that is *not* a subgroup.

Worked Exercise E9

Show that the subset

$$W = \left\{ \begin{pmatrix} a & 1 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\}$$

of $\text{GL}(2)$ is not a subgroup of $\text{GL}(2)$.

Solution

Subgroup property SG2 fails for W , because the identity element

$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of $\text{GL}(2)$ is not in W , since its top right entry is not 1.

Here are some similar exercises for you to try.

Exercise E21

Show that the following are groups under matrix multiplication, by showing that they are subgroups of $\text{GL}(2)$.

(a) $M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}$

(b) $P = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} : a \in \mathbb{R}, a \neq 0 \right\}$

Exercise E22

Show that the subset

$$X = \left\{ \begin{pmatrix} a & b \\ c & 1 \end{pmatrix} : a, b, c \in \mathbb{R}, a - bc \neq 0 \right\}$$

of $\text{GL}(2)$ is not a subgroup of $\text{GL}(2)$.

The group $\text{GL}(2)$ also has non-trivial *finite* subgroups. For example, you saw in Exercise E3 in Subsection 1.1 that the set of matrices $\{\mathbf{I}, \mathbf{R}, \mathbf{S}, \mathbf{T}\}$ is a group under matrix multiplication, where

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{R} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{S} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Each of these matrices is in $\text{GL}(2)$, since each of them has a non-zero determinant.

3 Group structures

This section contains revision of four topics from Book B that relate to the structures of groups, namely the *order of a group element*, *cyclic subgroups*, *cyclic groups* and *isomorphic groups*.

3.1 Order of a group element

In this first subsection you will revise the idea of the *order* of a group element. This is a different concept from the order of a *group*, which as you have seen means the number of elements in the group.

First, here is a reminder about *multiplicative notation* and *additive notation*.

We use **multiplicative notation** for abstract groups (such as the general groups mentioned in theorems, proofs and general discussions about groups) and for groups whose binary operation is some kind of multiplication, or function composition. We call such groups **multiplicative groups**.

We use **additive notation** for groups whose binary operation is some kind of addition, and we call such groups **additive groups**.

The box below summarises the two types of notation.

| Multiplicative notation and additive notation for groups | | |
|--|---|-------------------------|
| Feature | Multiplicative notation | Additive notation |
| Composite | $a \circ b$ or $a \times b$ or ab (or similar) | $a + b$ (or similar) |
| Identity | e or 1 | 0 |
| Inverse | x^{-1} | $-x$ |
| Power/multiple | x^n | nx |

The last row of the table in the box above relates to the following conventions.

If we repeatedly compose an element x of a *multiplicative* group with itself, then we call the resulting element a **power** of x , as follows.

Definition

Powers of an element x of a multiplicative group (G, \circ) are defined as follows. Let n be a positive integer. Then

$$\begin{aligned} x^0 &= e, \quad \text{the identity element} \\ x^n &= \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ copies of } x} \\ x^{-n} &= \underbrace{x^{-1} \circ x^{-1} \circ \cdots \circ x^{-1}}_{n \text{ copies of } x^{-1}}. \end{aligned}$$

All powers of x are elements of G , since G is closed under \circ .

If we repeatedly compose an element x of an *additive* group with itself, then we call the resulting element a **multiple** of x , as follows.

Definition

Multiples of an element x of an additive group $(G, +)$ are defined as follows. Let n be a positive integer. Then

$$\begin{aligned} 0x &= e, \quad \text{the identity element} \\ nx &= \underbrace{x + x + \cdots + x}_{n \text{ copies of } x} \\ -nx &= \underbrace{(-x) + (-x) + \cdots + (-x)}_{n \text{ copies of } -x}. \end{aligned}$$

All multiples of x are elements of G , since G is closed under $+$.

Most results and discussions in group theory are stated in multiplicative notation. To apply them to an additive group, you have to translate them into additive notation.

For example, the following boxes state the index laws for group elements and the versions obtained when they are translated into additive notation. You met these laws in Unit B2.

Theorem B27 Index laws

Let x be an element of a group (G, \circ) , and let m and n be integers. The following index laws hold.

- (a) $x^m \circ x^n = x^{m+n}$
- (b) $(x^m)^n = x^{mn}$
- (c) $(x^n)^{-1} = x^{-n} = (x^{-1})^n$

Theorem B28 Index laws (in additive notation)

Let x be an element of a group $(G, +)$, and let m and n be integers. The following laws hold.

- (a) $mx + nx = (m + n)x$
- (b) $n(mx) = (nm)x$
- (c) $-(nx) = (-n)x = n(-x)$

Usually group theory results and discussions will not be explicitly translated into additive notation for you, as that would complicate and lengthen the text. Occasionally the versions in additive notation are given for clarity, but most often you will have to do the translation yourself as needed.

Exercise E23

Translate the following statements about an element x of a multiplicative group (G, \circ) into additive notation for an element x of an additive group $(G, +)$.

- (a) $x^3 \circ x = x^4$
- (b) $x^5 \circ x^{-5} = e$
- (c) $(x^4)^{-1} = (x^{-1})^4$

We can now define what is meant by the *order of a group element*.

Definitions

Let x be an element of a group (G, \circ) .

If there is a positive integer n such that $x^n = e$, then the **order** of x is the *smallest* positive integer n such that $x^n = e$. We say that x has **finite order**.

If there is no positive integer n such that $x^n = e$, then x has **infinite order**.

Worked Exercise E10

Determine the order of each of the following group elements.

- (a) c in $S(\square)$ (shown in Figure 16) (b) 2 in (\mathbb{R}^*, \times)

Solution

- (a) In $S(\square)$ we have

$$\begin{aligned}c^1 &= c, \\c^2 &= c \circ c = b, \\c^3 &= c^2 \circ c = b \circ c = a, \\c^4 &= c^3 \circ c = a \circ c = e.\end{aligned}$$

☁ We have shown that the *smallest* positive integer n such that $c^n = e$ is 4. ☁

Thus c has order 4 in $S(\square)$.

- (b) ☁ We have

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad \dots$$

No matter how long we keep going we will not reach a positive integer n such that 2^n is equal to the identity element 1 of (\mathbb{R}^*, \times) . ☁

There is no positive integer n such that $2^n = 1$, so 2 has infinite order in (\mathbb{R}^*, \times) .

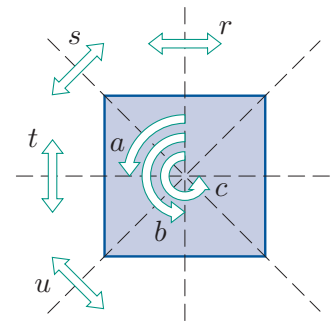


Figure 16 $S(\square)$

You met the following results in Unit B2.

Orders of elements in finite and infinite groups

- In every group, the identity element e has order 1.
- If the group element x is self-inverse and $x \neq e$, then x has order 2.

Theorem B29 Every element of a finite group has finite order.

Theorem B30 A group element and its inverse either have the same finite order, or they both have infinite order.

Exercise E24

Determine the order of each of the following group elements.

- (a) In $S(\square)$: (i) a (ii) b (iii) r
 (b) In (U_9, \times_9) : (i) 5 (ii) 2 (iii) 7
 (c) In $(\mathbb{Z}_8, +_8)$: (i) 2 (ii) 3 (iii) 6

Exercise E25

Find the order of each of the following elements of the group $GL(2)$.

(a) $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

You met the following important theorem in Unit B2. Part (a) of the theorem is illustrated in Figure 17.

Theorem B31

Let x be an element of a group (G, \circ) .

(a) If x has finite order n , then the n powers

$$e, x, x^2, \dots, x^{n-1}$$

are distinct, and these elements repeat indefinitely every n powers in the list of consecutive powers of x .

(b) If x has infinite order, then all the powers of x are distinct.

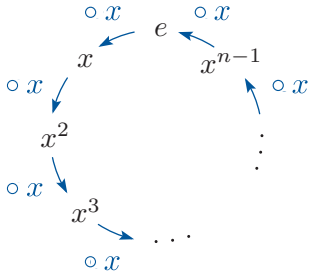


Figure 17 The cycle of powers of an element x of order n

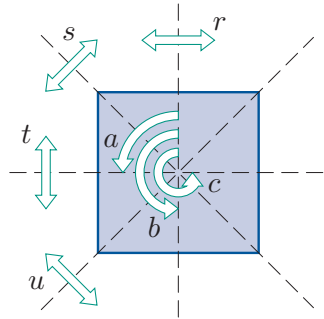


Figure 18 $S(\square)$

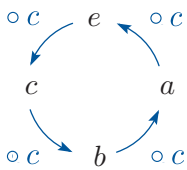


Figure 19 The cycle of powers of the element c in $S(\square)$

For example, in $S(\square)$ (see Figure 18), the element c has order 4, and the list of consecutive powers of c in $S(\square)$ (including the zeroth power and the negative powers) is

$$\dots, c^{-4}, c^{-3}, c^{-2}, c^{-1}, c^0, c^1, c^2, c^3, c^4, c^5, c^6, c^7, c^8, \dots,$$

which evaluates to

$$\dots, e, c, b, a, e, c, b, a, e, c, b, a, \dots$$

So the powers e, c, c^2, c^3 , that is, e, c, b, a , repeat indefinitely every 4 powers, as shown in Figure 19.

You met another important theorem about the orders of group elements in Unit B4.

Corollary B69 to Lagrange's Theorem

Let g be an element of a finite group G . Then the order of g divides the order of G .

Finally in this subsection, let us look at how to find the order of an element of a symmetric group, that is, the order of a permutation. One method is to find its consecutive powers, as for any group element, but there is a much quicker method, as follows.

Order of a permutation in cycle form

The order of a permutation in cycle form is the least common multiple of the lengths of its cycles.

For example, the permutation $(1\ 3\ 4)(2\ 6)(5\ 9\ 7\ 8)$ in S_9 has cycles of lengths 3, 2 and 4, so its order is the least common multiple of 3, 2 and 4, which is 12.

Exercise E26

State the orders of the following permutations in S_9 .

- (a) $(2\ 3)(6\ 9\ 8)$ (b) $(1\ 7\ 3\ 2\ 4)$ (c) $(1\ 7)(3\ 6\ 4\ 5)$

3.2 Cyclic subgroups

If x is an element of a group (G, \circ) , then we denote the set of all powers of x (including the zeroth power and all negative powers) by $\langle x \rangle$. That is,

$$\langle x \rangle = \{x^k : k \in \mathbb{Z}\}.$$

In the case of an element x of an *additive* group $(G, +)$, the set $\langle x \rangle$ is the set of all multiples of x :

$$\langle x \rangle = \{kx : k \in \mathbb{Z}\}.$$

The theorem below was proved in Unit B2.

Theorem B32

Let x be an element of a group (G, \circ) . Then $(\langle x \rangle, \circ)$ is a subgroup of (G, \circ) .

The subgroup $(\langle x \rangle, \circ)$ in Theorem B32 is called the **cyclic subgroup of (G, \circ) generated by x** . It may contain infinitely many elements, or, if the powers (or multiples) of x are not all distinct, only finitely many elements.

For example, in $S(\square)$, whose non-identity elements are shown in Figure 20, the powers of the element c are

$$\dots, e, c, b, a, e, c, b, a, e, c, b, a, \dots,$$

so

$$\langle c \rangle = \{e, a, b, c\}.$$

Similarly, in $(\mathbb{Z}_9, +_9)$ the multiples of the element 3 are

$$\dots, 0, 3, 6, 0, 3, 6, 0, 3, 6, \dots,$$

so

$$\langle 3 \rangle = \{0, 3, 6\}.$$

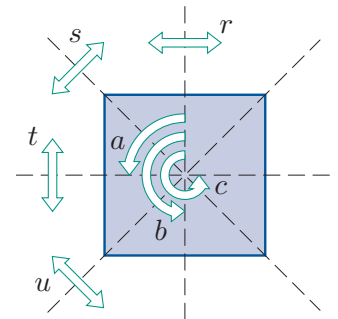


Figure 20 $S(\square)$

In $(\mathbb{Z}, +)$ the multiples of the element 7 are

$$\dots, -21, -14, -7, 0, 7, 14, 21, \dots$$

(there is no repeating pattern), so

$$\langle 7 \rangle = \{\dots, -21, -14, -7, 0, 7, 14, 21, \dots\}.$$

These examples illustrate the following theorem.

Theorem B33

Let x be an element of a group (G, \circ) .

(a) If x has finite order n , then the subgroup $\langle x \rangle$ has order n .

In multiplicative notation,

$$\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}.$$

In additive notation,

$$\langle x \rangle = \{0, x, 2x, \dots, (n-1)x\}.$$

(b) If x has infinite order, then the subgroup $\langle x \rangle$ has infinite order.

In multiplicative notation,

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}.$$

In additive notation,

$$\langle x \rangle = \{\dots, -2x, -x, 0, x, 2x, \dots\}.$$

Theorem B33 shows in particular that there is a close connection between the two meanings of the word *order* in group theory: the order of an element x is equal to the order of the cyclic subgroup generated by x . For example, in $S(\square)$ the element c has order 4 and the subgroup

$$\langle c \rangle = \{e, c, c^2, c^3\} = \{e, a, b, c\}$$

has order 4.

Exercise E27

By using the solution to Exercise E24, determine the cyclic subgroup generated by each of the following group elements.

- (a) In $S(\square)$: (i) a (ii) b (iii) r
 (b) In (U_9, \times_9) : (i) 5 (ii) 2 (iii) 7
 (c) In $(\mathbb{Z}_8, +_8)$: (i) 2 (ii) 3 (iii) 6

Two different elements of a group can generate the same cyclic subgroup. For example, in $S(\square)$ the elements a and c do this:

$$\begin{aligned}\langle a \rangle &= \{e, a, a^2, a^3\} = \{e, a, b, c\}, \\ \langle c \rangle &= \{e, c, c^2, c^3\} = \{e, c, b, a\} = \{e, a, b, c\} = \langle a \rangle.\end{aligned}$$

You saw other examples of this in Exercise E27.

The following simple results about cyclic subgroups were proved in Subsection 3.1 of Unit B2.

Some special cyclic subgroups

Let (G, \circ) be a group with identity element e , and let $x \in G$.

- $\langle e \rangle = \{e\}$.
- If x is self-inverse and $x \neq e$, then $\langle x \rangle = \{e, x\}$.
- $\langle x^{-1} \rangle = \langle x \rangle$ (or, in additive notation, $\langle -x \rangle = \langle x \rangle$).

Exercise E28

For each of the following groups, determine the cyclic subgroup generated by each of its elements, and list the distinct cyclic subgroups of the group, stating how many there are.

- (a) $S(\square)$ (b) $(\mathbb{Z}_9, +_9)$ (c) $(\mathbb{Z}_7^*, \times_7)$ (d) S_3

3.3 Cyclic groups

We make the following definitions.

Definitions

A group G is **cyclic** if it contains an element x such that $G = \langle x \rangle$. Such an element x is called a **generator** of the group.

A group that is not cyclic is called **non-cyclic**.

For example, in $(\mathbb{Z}_9, +_9)$,

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \mathbb{Z}_9,$$

so $(\mathbb{Z}_9, +_9)$ is a cyclic group, and 1 is a generator of this group. In fact, the elements 2, 4, 5, 7 and 8 are also generators of $(\mathbb{Z}_9, +_9)$, as you can see from the solution to Exercise E28(b).

The theorem below follows immediately from the fact that a group element of order n generates a cyclic subgroup of order n (Theorem B33(a)).

Theorem B34

A finite group of order n is cyclic if and only if it contains an element of order n .

Exercise E29

Determine which of the following groups are cyclic. State all the generators of each cyclic group.

- (a) $S(\square)$ (b) $S^+(\square)$ (c) $(\mathbb{Z}_5, +_5)$ (d) (U_8, \times_8)

In Unit B2 you met the following theorems about cyclic groups.

Theorem B35 Every cyclic group is abelian.

Theorem B36 Every subgroup of a cyclic group is cyclic.

You also studied the standard cyclic groups $(\mathbb{Z}_n, +_n)$, where $n \geq 2$, in detail, and met the following theorems.

The group $(\mathbb{Z}_n, +_n)$ ($n \geq 2$)

Theorem B37 The group $(\mathbb{Z}_n, +_n)$ is cyclic, and one of its generators is 1.

Theorem B38 If m is a non-zero element of $(\mathbb{Z}_n, +_n)$, then m has order n/d , where d is the highest common factor of m and n .

Corollary B40 The element m of $(\mathbb{Z}_n, +_n)$ is a generator of $(\mathbb{Z}_n, +_n)$ if and only if m is coprime to n .

Exercise E30

- (a) Find the order of each element of the group $(\mathbb{Z}_{14}, +_{14})$.
(b) State the generators of the group $(\mathbb{Z}_{14}, +_{14})$.

The following theorem describes all the subgroups of each group $(\mathbb{Z}_n, +_n)$, where $n \geq 2$.

Theorem B41 Subgroups of $(\mathbb{Z}_n, +_n)$

The group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order q for each positive factor q of n , and no other subgroups.

- The subgroup of order 1 is generated by 0.
- For each other factor q of n , the subgroup of order q is generated by d , where $qd = n$.

Exercise E31

Write down all the distinct cyclic subgroups of the group $(\mathbb{Z}_{16}, +_{16})$, listing the elements of each subgroup and giving each subgroup once only.

3.4 Isomorphic groups

In this subsection we will revise what it means for two groups to be *isomorphic*.

Consider the five groups of order 4 whose group tables are given below.

| \circ | e | a | b | c |
|---------|-----|-----|-----|-----|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

$(S^+(\square), \circ)$

| $+_4$ | 0 | 1 | 2 | 3 |
|-------|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

$(\mathbb{Z}_4, +_4)$

| \times_5 | 1 | 2 | 3 | 4 |
|------------|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

$(\mathbb{Z}_5^*, \times_5)$

| \circ | e | a | r | s |
|---------|-----|-----|-----|-----|
| e | e | a | r | s |
| a | a | e | s | r |
| r | r | s | e | a |
| s | s | r | a | e |

$(S(\square), \circ)$

| \times_8 | 1 | 3 | 5 | 7 |
|------------|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

(U_8, \times_8)

In one sense, all these groups are different, because their sets and binary operations are different. Superficially, they have a ‘sameness’ in that they all have four elements. The idea of isomorphism is much stronger than this: two groups are **isomorphic** if they have identical structures – that is, if one of the groups can be obtained from the other by ‘renaming’ the elements and the binary operation.

For finite groups we can define this concept more rigorously as follows: two finite groups are *isomorphic* if there is a one-to-one and onto mapping from one group to the other group that transforms a group table for the first group into a group table for the second group. Such a mapping is called an **isomorphism**. (The isomorphism ‘renames’ the elements.) Remember that ‘mapping’ is just another word for ‘function’.

For example, consider the first two of the five groups above, $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$, whose group tables are repeated below.

| \circ | e | a | b | c |
|---------|-----|-----|-----|-----|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

$(S^+(\square), \circ)$

| $+_4$ | 0 | 1 | 2 | 3 |
|-------|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

$(\mathbb{Z}_4, +_4)$

If we take the group table of $(S^+(\square), \circ)$ and replace each element in it with an element of $(\mathbb{Z}_4, +_4)$ according to the ‘renaming’ mapping

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_4 \\ e &\longmapsto 0 \\ a &\longmapsto 1 \\ b &\longmapsto 2 \\ c &\longmapsto 3 \end{aligned}$$

(and also replace the symbol \circ in the table with the symbol $+_4$), then we obtain the group table of $(\mathbb{Z}_4, +_4)$, as you can check. So these two groups are isomorphic, and the mapping ϕ is an isomorphism.

The reason why the group table of $(\mathbb{Z}_4, +_4)$ can be obtained from the group table of $(S^+(\square), \circ)$ by ‘renaming’ the elements is that the two group tables have exactly the same pattern. They both have the pattern of bottom left to top right diagonal stripes shown in Figure 21.

Now consider the third of the five groups above, $(\mathbb{Z}_5^*, \times_5)$. At first sight it looks as if it has a structure different from that of the first two groups, because its group table does not have the pattern of diagonal stripes in Figure 21. However, if we swap the elements 3 and 4 in the borders of the group table of $(\mathbb{Z}_5^*, \times_5)$, and rearrange the entries in the body of the table accordingly so that the table is still a correct group table for $(\mathbb{Z}_5^*, \times_5)$, then we obtain the following table:

| \times_5 | 1 | 2 | 4 | 3 |
|------------|---|---|---|---|
| 1 | 1 | 2 | 4 | 3 |
| 2 | 2 | 4 | 3 | 1 |
| 4 | 4 | 3 | 1 | 2 |
| 3 | 3 | 1 | 2 | 4 |



Figure 21 The pattern of the group tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$

This group table for $(\mathbb{Z}_5^*, \times_5)$ does have the pattern of diagonal stripes in Figure 21, so the group $(\mathbb{Z}_5^*, \times_5)$ is isomorphic to the first two groups. The following mapping, obtained by matching up the elements in the borders of the group table for $(S^+(\square), \circ)$ and the rearranged group table for $(\mathbb{Z}_5^*, \times_5)$, is an isomorphism:

$$\begin{aligned}\phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 1 \\ a &\longmapsto 2 \\ b &\longmapsto 4 \\ c &\longmapsto 3.\end{aligned}$$

Now consider the final two of the five groups above, $(S(\square), \circ)$ and (U_8, \times_8) , whose group tables are repeated below.

| \circ | e | a | r | s | \times_8 | 1 | 3 | 5 | 7 |
|---------|-----|-----|-----|-----|------------|---|---|---|---|
| e | e | a | r | s | 1 | 1 | 3 | 5 | 7 |
| a | a | e | s | r | 3 | 3 | 1 | 7 | 5 |
| r | r | s | e | a | 5 | 5 | 7 | 1 | 3 |
| s | s | r | a | e | 7 | 7 | 5 | 3 | 1 |

$(S(\square), \circ)$
 (U_8, \times_8)



Figure 22 The pattern of the group tables of $(S(\square), \circ)$ and (U_8, \times_8)

These group tables have the same pattern as each other, namely the pattern shown in Figure 22, so these two groups are certainly isomorphic to each other.

To determine whether they are also isomorphic to the first three groups, we need to ascertain whether it is possible to rearrange the elements in the borders of their group tables to obtain group tables that have the diagonal stripes pattern in Figure 21. A little thought shows that this is *not* possible: in each of these two groups every element is self-inverse, so no matter how we rearrange the borders of their group tables, the four positions on the main diagonal will contain four occurrences of the identity element, whereas the diagonal stripes pattern has two different elements on the main diagonal. So the groups $(S(\square), \circ)$ and (U_8, \times_8) are *not* isomorphic to the groups $(S^+(\square), \circ)$, $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \times_5)$.

Exercise E32

- List the elements of the group (U_{10}, \times_{10}) .
- Construct a group table for this group.
- Show that (U_{10}, \times_{10}) is isomorphic to one of $(\mathbb{Z}_4, +_4)$ or $(S(\square), \circ)$ by finding an isomorphism from (U_{10}, \times_{10}) to one of these two groups.

You saw above that the condition for a one-to-one and onto mapping ϕ from a finite group (G, \circ) to a finite group $(H, *)$ to be an isomorphism is that it must transform the group table of (G, \circ) into a group table for $(H, *)$. This condition can be expressed algebraically as follows.

Consider any elements x and y of G , and their composite $x \circ y$ in the group table for (G, \circ) , as illustrated on the left below. In the table transformed by using the mapping ϕ , these three elements are replaced by $\phi(x)$, $\phi(y)$ and $\phi(x \circ y)$, as illustrated on the right.

| | | | | | | | | |
|--------------|----------|-------------|----------|-------------------|-----------|----------|-------------------|----------|
| \circ | \cdots | y | \cdots | | $*$ | \cdots | $\phi(y)$ | \cdots |
| \vdots | | \vdots | | | \vdots | | \vdots | |
| x | \cdots | $x \circ y$ | \cdots | \longrightarrow | $\phi(x)$ | \cdots | $\phi(x \circ y)$ | \cdots |
| \vdots | | \vdots | | | \vdots | | \vdots | |
| (G, \circ) | | | | | $(H, *)$ | | | |

If the table obtained is to be a correct group table for $(H, *)$, then the entry in the cell with row label $\phi(x)$ and column label $\phi(y)$ must be equal to $\phi(x) * \phi(y)$, so we must have

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

This applies to all elements x and y of G , so the condition for ϕ to be an isomorphism can be expressed algebraically as

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G.$$

Thus we can define an isomorphism from a finite group (G, \circ) to a finite group $(H, *)$ to be a one-to-one and onto mapping $\phi : (G, \circ) \longrightarrow (H, *)$ that satisfies the condition above. This also applies to *infinite* groups; the only difference is that we cannot write down group tables for such groups. So we have the following definitions.

Definitions

Two groups (G, \circ) and $(H, *)$ are **isomorphic** if there exists a mapping $\phi : G \longrightarrow H$ with the following properties.

- (a) ϕ is one-to-one and onto.
- (b) For all $x, y \in G$,

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

Such a mapping ϕ is called an **isomorphism**.

We write $(G, \circ) \cong (H, *)$ to assert that the groups (G, \circ) and $(H, *)$ are isomorphic.

Exercise E33

The cyclic subgroup of the infinite additive group $(\mathbb{Z}, +)$ generated by the integer 3 is

$$\langle 3 \rangle = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\},$$

and we denote this group by $3\mathbb{Z}$. Show that $(\mathbb{Z}, +) \cong (3\mathbb{Z}, +)$ by showing that the mapping

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow 3\mathbb{Z} \\ n &\longmapsto 3n\end{aligned}$$

is an isomorphism.

The collection of all groups can be split (*partitioned*) into disjoint classes, which we call **isomorphism classes**, such that two groups belong to the same isomorphism class if they are isomorphic, and belong to different isomorphism classes otherwise.

Within each isomorphism class all the groups have the same order, since two groups cannot be isomorphic if they do not have the same order. However, two groups of the same order may not be isomorphic, so there may be more than one isomorphism class for groups of a particular order.

Earlier in this subsection you saw two different structures for groups of order 4. It was proved in Subsection 2.3 of Unit B4 that these two structures are the only possible structures for groups of order 4, so there are exactly two isomorphism classes for groups of order 4.

In fact you met all the isomorphism classes for groups of orders 1 to 8 in Section 2 of Unit B4. They are summarised in the table below. There is a row for each different isomorphism class, so the table shows that for each of the orders 1, 2, 3, 5 and 7 there is just one isomorphism class, whereas for each of the orders 4 and 6 there are two isomorphism classes, and for order 8 there are five isomorphism classes.

For each isomorphism class, the table gives one or two standard groups in the class. Where there is more than one isomorphism class for groups of a particular order, the table gives some distinguishing features of groups in the different classes. For example the table shows that if a group of order 6 is abelian (or contains an element of order 6), then it is isomorphic to the group C_6 (and to the group \mathbb{Z}_6).

Recall that the notation C_n , where n is a positive integer, denotes a standard, abstract cyclic group of order n . The notation V denotes the *Klein four-group*, which is a standard, abstract group isomorphic to $S(\square)$, the symmetry group of a rectangle. The notation Q_8 denotes the *quaternion group*, a group of order 8 that contains an identity element, one element of order 2 and six elements of order 4; its group table was given in Subsection 2.5 of Unit B4. The group $S(\text{cuboid})$ is the symmetry group of a cuboid with no square faces.

Isomorphism classes for groups of orders 1 to 8

| Order | Standard group(s) | Distinguishing features (given the order of the group) |
|-------|---------------------|---|
| 1 | C_1 | |
| 2 | C_2, \mathbb{Z}_2 | |
| 3 | C_3, \mathbb{Z}_3 | |
| 4 | C_4, \mathbb{Z}_4 | Exactly 2 self-inverse elements. An element of order 4. |
| | $V, S(\square)$ | All elements self-inverse. |
| 5 | C_5, \mathbb{Z}_5 | |
| 6 | C_6, \mathbb{Z}_6 | Abelian. An element of order 6. |
| | $S(\triangle)$ | Non-abelian. |
| 7 | C_7, \mathbb{Z}_7 | |
| 8 | C_8, \mathbb{Z}_8 | Abelian with exactly 2 self-inverse elements. An element of order 8. |
| | $S(\text{cuboid})$ | Abelian with all elements self-inverse. |
| | U_{15} | Abelian with exactly 4 self-inverse elements. |
| | $S(\square)$ | Non-abelian with exactly 6 self-inverse elements. |
| | Q_8 | Non-abelian with exactly 2 self-inverse elements. |

Where two sets of distinguishing features are given on separate lines in the same row of the table, either distinguishes the isomorphism class.

Notice that the table does not state the binary operation of the standard groups. You are familiar with a symmetry group $(S(F), \circ)$ being denoted by just $S(F)$. In the same way, we will often use the following abbreviated notation throughout the rest of this book.

- The group \mathbb{Z}_n means the group $(\mathbb{Z}_n, +_n)$.
- The group U_n means the group (U_n, \times_n) .
- The group \mathbb{Z}_p^* means the group $(\mathbb{Z}_p^*, \times_p)$ (where p is prime).

These assumptions are natural: \mathbb{Z}_n is a group under $+_n$ but not under \times_n , U_n is a group under \times_n but not under $+_n$, and (provided p is prime) \mathbb{Z}_p^* is a group under \times_p but not under $+_p$.

Exercise E34

State a standard group that is isomorphic to the group (G, \times) of matrices whose group table you were asked to find in Exercise E3 in Subsection 1.1, justifying your answer.

Exercise E35

Write down the elements of the group U_{18} . Without constructing a group table for this group, identify a standard group from the table of isomorphism classes above that is isomorphic to this group, justifying your answer.

The table of isomorphism classes in the box above indicates that there is only one isomorphism class for each of the orders 2, 3, 5 and 7. In fact there is only one isomorphism class for any prime order. This follows from the corollary below.

Corollary B71 to Lagrange's Theorem

If G is a group of prime order p , then G is isomorphic to the cyclic group $(\mathbb{Z}_p, +_p)$.

You will revise isomorphisms further in Unit E3 *Homomorphisms*.

You have now finished the revision of Book B in this unit. In the rest of the unit you will be studying new material.

4 Cosets

In this section you will see how we can use a subgroup of a group to split the group in a natural way into disjoint subsets, one of which is the subgroup itself. You have already seen some examples of this. For instance, the group $S(\square)$ can be split into its subgroup of direct symmetries and its subset of indirect symmetries, as follows:

$$S(\square) = \{e, a, b, c\} \cup \{r, s, t, u\}.$$

Another example is that the group \mathbb{Z}_{12} (that is, $(\mathbb{Z}_{12}, +_{12})$) can be split into its subgroup $\langle 4 \rangle = \{0, 4, 8\}$ and three other subsets obtained by ‘shifting’ this subgroup, that is, by adding (modulo 12) the same element of \mathbb{Z}_{12} to each element of the subgroup:

$$\mathbb{Z}_{12} = \{0, 4, 8\} \cup \{1, 5, 9\} \cup \{2, 6, 10\} \cup \{3, 7, 11\}.$$

The second subset here is obtained by adding 1 to each element of the subgroup, the third subset by adding 2 and the fourth subset by adding 3.

In each of these two examples, the subsets are *cosets*, which you will learn about in this section.

Cosets are of fundamental importance in group theory. They are of two types: *left cosets* and *right cosets*. In the first subsection we will look at left cosets. Right cosets are similar and are dealt with in the second subsection.

Note that although so far in this unit we have usually denoted an abstract group by (G, \circ) , and a composite of two elements x and y of G by $x \circ y$, for the remainder of the unit and in the rest of Book E we will often adopt the following useful convention, which you met in Unit B4.

Convention

In discussions about abstract groups, we use the following notation and terminology where it will not cause confusion.

- We denote an abstract group simply by a single symbol such as G , without specifying a symbol for its binary operation.
- We denote a composite of two elements x and y of G simply by xy .

Warning: Unless the group is abelian, the composites xy and yx are not necessarily equal.

We refer to multiplicative notation that uses this convention as *concise multiplicative notation*.

4.1 Left cosets

We begin with the definition of a *left coset*.

Definition

Let H be a subgroup of a group G , and let g be an element of G . The **left coset** gH of H is given by

$$gH = \{gh : h \in H\}.$$

It is the subset of G obtained by composing each element of H with g on the left.

This definition is expressed in the concise multiplicative notation described in the convention above, so you may need to translate it when you want to apply it to a particular group. For example, consider the subgroup $H = \langle r \rangle = \{e, r\}$ of the group $S(\square)$, and the element a of $S(\square)$. The left coset aH of H in $S(\square)$ is

$$aH = a\{e, r\} = \{a \circ e, a \circ r\} = \{a, s\}.$$

Notice that, for brevity, we usually denote a left coset by notation of the form gH , not $g \circ H$, even if we are using the symbol \circ to denote the binary operation.

The word ‘left’ in ‘left coset’ refers to the fact that to obtain the left coset gH we compose each element of H with g on the left. *Right cosets* are obtained in a similar way but by composing on the right; you will study them in the next subsection.

You can think of a coset (either left or right) of a subgroup as being obtained by ‘shifting’ the subgroup, in the sense that to obtain the left coset gH , for example, we ‘shift’ every element of the subgroup H in the same way, by composing it with the group element g on the left. This is illustrated in Figure 23.

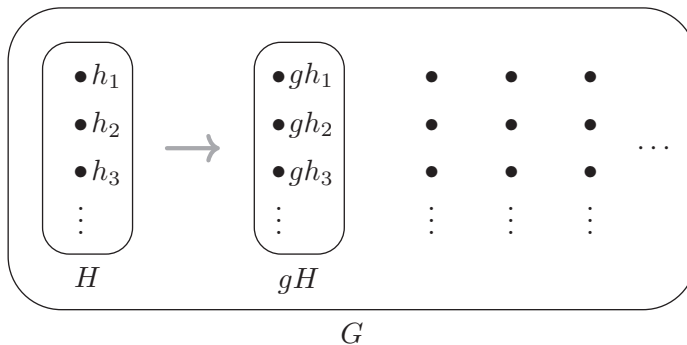


Figure 23 A left coset of a subgroup H in a group G is a ‘shift’ of H

In the next worked exercise we find *all* the left cosets of the subgroup $H = \{e, r\}$ of the group $S(\square)$, by calculating the left coset gH for each element g in $S(\square)$ in turn.

Worked Exercise E11

Find all the left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$. (The group table of $S(\square)$ is given as Table 5.)

Table 5 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

Solution

For each $g \in S(\square)$, we calculate the left coset gH .

$$\begin{aligned}
 eH &= e\{e, r\} = \{e \circ e, e \circ r\} = \{e, r\}, \\
 aH &= a\{e, r\} = \{a \circ e, a \circ r\} = \{a, s\}, \\
 bH &= b\{e, r\} = \{b \circ e, b \circ r\} = \{b, t\}, \\
 cH &= c\{e, r\} = \{c \circ e, c \circ r\} = \{c, u\}, \\
 rH &= r\{e, r\} = \{r \circ e, r \circ r\} = \{r, e\}, \\
 sH &= s\{e, r\} = \{s \circ e, s \circ r\} = \{s, a\}, \\
 tH &= t\{e, r\} = \{t \circ e, t \circ r\} = \{t, b\}, \\
 uH &= u\{e, r\} = \{u \circ e, u \circ r\} = \{u, c\}.
 \end{aligned}$$

Notice from Worked Exercise E11 that a left coset of a subgroup is not necessarily a subgroup itself.

Notice also that some of the left cosets found in Worked Exercise E11 turn out to be the same set. For example, both eH and rH are the set $\{e, r\}$. In fact there are only four *distinct* left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$, because

$$\begin{aligned}
 eH &= rH = \{e, r\}, \\
 aH &= sH = \{a, s\}, \\
 bH &= tH = \{b, t\}, \\
 cH &= uH = \{c, u\}.
 \end{aligned}$$

So the distinct left cosets of $H = \{e, r\}$ in $S(\square)$ are

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

Exercise E36

- Find all the left cosets of the subgroup $H = \{e, s\}$ in the group $S(\triangle)$. (The group table of $S(\triangle)$ is given as Table 6.)
- List the distinct left cosets of $H = \{e, s\}$ in $S(\triangle)$.

Exercise E37

- Show that $H = \{1, 2, 4\}$ is a subgroup of the group \mathbb{Z}_7^* . (Remember that we use \mathbb{Z}_7^* to denote the group $(\mathbb{Z}_7^*, \times_7)$.)
- Find all the left cosets of H in \mathbb{Z}_7^* .
- List the distinct left cosets of H in \mathbb{Z}_7^* .

Table 6 $S(\triangle)$

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

You saw just after Worked Exercise E11 that the distinct left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$ are

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

Notice that these sets form a *partition* of the group $S(\square)$, as illustrated in Figure 24. Remember that a **partition** of a set is a family of subsets of the set such that every element of the set belongs to one of the subsets, and each pair of the subsets are **disjoint** – that is, they have no elements in common. In other words, each element of the set belongs to *exactly one* of the subsets in the partition.

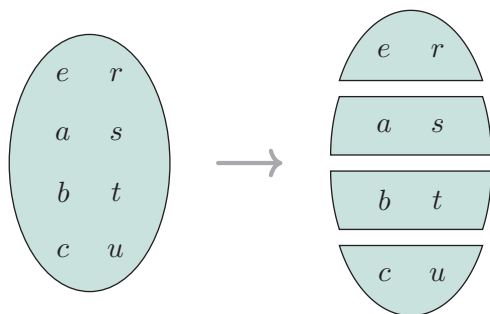


Figure 24 The group $S(\square)$ partitioned into the left cosets of the subgroup $\{e, r\}$

Similarly, in each of Exercises E36 and E37 you should have found that the distinct left cosets of the subgroup form a partition of the group, as illustrated in Figure 25.

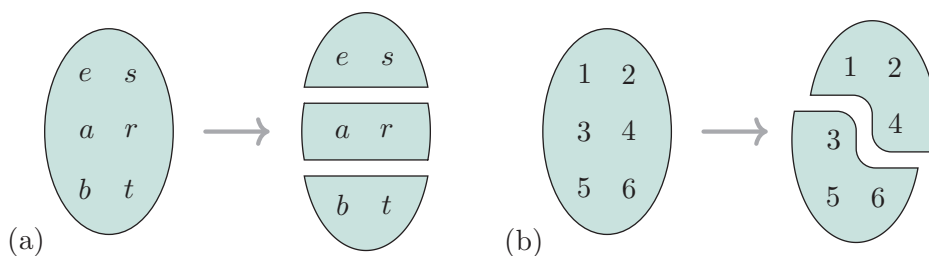


Figure 25 Groups partitioned into left cosets of a subgroup: (a) $S(\triangle)$ with subgroup $\{e, s\}$ (b) \mathbb{Z}_7^* with subgroup $\{1, 2, 4\}$

In fact, this always happens, as stated in the next theorem.

Theorem E2

Let H be a subgroup of a group G . Then the distinct left cosets of H in G form a partition of G .

To prove this theorem we use the properties of equivalence relations, which you met in Unit A3 *Mathematical language and proof*. Remember that \sim is a *relation* on a set X if, whenever $x, y \in X$, the statement $x \sim y$ is either true or false, and an *equivalence relation* is a relation with the properties in the definition below.

Definition

A relation \sim on a set X is an **equivalence relation** if it has the following three properties.

E1 Reflexivity For all x in X ,

$$x \sim x.$$

E2 Symmetry For all x, y in X ,

$$\text{if } x \sim y, \text{ then } y \sim x.$$

E3 Transitivity For all x, y, z in X ,

$$\text{if } x \sim y \text{ and } y \sim z, \text{ then } x \sim z.$$

As you saw in Unit A3, if \sim is an equivalence relation on a set X and $x \in X$, then we call the set $\{y \in X : x \sim y\}$ the **equivalence class** of x and denote it by $\llbracket x \rrbracket$. The key property of equivalence classes that we need is the following result from Unit A3.

Theorem A16

The equivalence classes of an equivalence relation on a set X form a partition of the set X .

We now apply these ideas to prove Theorem E2, which is repeated below. The overall method of the proof is that we define a particular relation on the set G , prove that it is an equivalence relation, and prove that its equivalence classes are the left cosets of H in G . It then follows from Theorem A16 that these left cosets form a partition of G .

Theorem E2

Let H be a subgroup of a group G . Then the distinct left cosets of H in G form a partition of G .

Proof Let \sim be the relation defined on G by

$$x \sim y \quad \text{if } x \in yH.$$

We show that \sim is an equivalence relation.

E1 Reflexive property

Let $x \in G$. We have to show that $x \sim x$, that is, $x \in xH$. This is true, because

$$x = xe$$

and $e \in H$, since H is a subgroup. Hence $x \sim x$. Thus \sim is reflexive.

E2 Symmetric property

Let $x, y \in G$, and suppose that $x \sim y$, that is, $x \in yH$. We have to show that $y \sim x$, that is, $y \in xH$. Since $x \in yH$, we have

$$x = yh$$

for some $h \in H$. Composing both sides of this equation with h^{-1} on the right gives

$$xh^{-1} = yhh^{-1},$$

that is,

$$xh^{-1} = y.$$

Now $h^{-1} \in H$, since H is a subgroup, so this shows that $y \in xH$, that is, $y \sim x$. Thus \sim is symmetric.

E3 Transitive property

Let $x, y, z \in G$, and suppose that $x \sim y$ and $y \sim z$, that is, $x \in yH$ and $y \in zH$. We have to show that $x \sim z$, that is, $x \in zH$. Since $x \in yH$ and $y \in zH$, we have

$$x = yh_1 \quad \text{and} \quad y = zh_2$$

for some $h_1, h_2 \in H$. Using the second equation above to substitute for y in the first equation gives

$$x = zh_2h_1.$$

Now $h_2h_1 \in H$, since H is a subgroup, so this shows that $x \in zH$, that is, $x \sim z$. Thus \sim is transitive.

Hence \sim is an equivalence relation.

Each element x in G has equivalence class

$$\begin{aligned} \llbracket x \rrbracket &= \{y \in G : y \sim x\} \\ &= \{y \in G : y \in xH\} \\ &= xH. \end{aligned}$$

Thus the equivalence classes of \sim are the left cosets of H in G . It follows from Theorem A16 that the left cosets of H in G form a partition of G , as required. ■

Some simple but important properties of left cosets are given in the proposition below.

Proposition E3 Properties of left cosets

Let H be a subgroup of a group G .

- (a) The element g lies in the left coset gH , for each $g \in G$.
- (b) One of the left cosets of H in G is H itself.
- (c) Any two left cosets g_1H and g_2H are either the same set or are disjoint.
- (d) If H is finite, then each left coset gH has the same number of elements as H .

To illustrate these properties, consider again the left cosets of the subgroup $H = \{e, r\}$ of $S(\square)$, found in Worked Exercise E11:

$$\begin{aligned} eH &= rH = \{e, r\}, \\ aH &= sH = \{a, s\}, \\ bH &= tH = \{b, t\}, \\ cH &= uH = \{c, u\}. \end{aligned}$$

Observe that they have the following properties, corresponding to the properties listed in Proposition E3.

- (a) $e \in eH$, $r \in rH$, $a \in aH$, and so on.
- (b) One of the left cosets, namely eH (equal also to rH), is H itself.
- (c) Any two left cosets are either the same set or are disjoint.
- (d) Each left coset has two elements, the same number of elements as H .

Proof of Proposition E3

- (a) Let $g \in G$. Then g lies in the left coset gH , because

$$g = ge$$

and $e \in H$ since H is a subgroup.

- (b) The subgroup H is a left coset of H because

$$eH = \{eh : h \in H\} = \{h : h \in H\} = H.$$

- (c) This property follows immediately from Theorem E2.
- (d) Suppose that H has order m , with $H = \{h_1, h_2, \dots, h_m\}$. Let g be any element of G . Then

$$gH = \{gh_1, gh_2, \dots, gh_m\}.$$

The m elements of the left coset gH listed here are all distinct, because the Cancellation Laws (Proposition B15) tell us that if $gh_i = gh_j$ then $h_i = h_j$. Hence gH has m elements, the same number of elements as H . ■

Exercise E38

Using only the properties of left cosets in Proposition E3, list the distinct left cosets of each of the following subgroups H of $S(\square)$.

- (a) $H = \{e, a, b, c\}$ (b) $H = \{e\}$ (c) $H = S(\square)$

The properties in Proposition E3 give us the following efficient strategy for partitioning a *finite* group into left cosets.

Strategy E1

To partition a finite group G into left cosets of a subgroup H , do the following.

1. Take H as the first left coset.
2. Choose any element $g \in G$ not yet assigned to a left coset and determine the left coset gH to which g belongs.
3. Repeat step 2 until every element of G has been assigned to a left coset.

Strategy E1 is applied in the next worked exercise, in which the left cosets found in Worked Exercise E11 are found again, but this time more efficiently.

Worked Exercise E12

Partition the group $S(\square)$ into left cosets of the subgroup $H = \{e, r\}$. (The group table of $S(\square)$ is given as Table 7.)

Solution

We use Strategy E1.

The left cosets are as follows.

The first left coset is H itself.

$$H = \{e, r\}$$

Now we choose an element not in H , say a , and find aH .

$$aH = \{a \circ e, a \circ r\} = \{a, s\}$$

Next we choose an element not in H or aH , say b , and find bH .

$$bH = \{b \circ e, b \circ r\} = \{b, t\}$$

Now we choose an element not in H , aH or bH , say c , and find cH .

$$cH = \{c \circ e, c \circ r\} = \{c, u\}$$

Every element of $S(\square)$ has now been assigned to a left coset.

So the partition into left cosets is

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

Table 7 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

You can practise applying Strategy E1 in the next two exercises.

Table 8 $S(\triangle)$

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

Exercise E39

Write down the elements of the group U_{20} , show that $H = \{1, 19\}$ is a subgroup of this group, and partition U_{20} into left cosets of this subgroup.

Exercise E40

Partition $S(\triangle)$ into left cosets of the subgroup $H = \{e, t\}$. (The group table of $S(\triangle)$ is given as Table 8.)

In the next worked exercise a permutation group is partitioned into left cosets.

Worked Exercise E13

Partition the group S_3 into left cosets of the subgroup

$$H = \langle (1, 2) \rangle = \{e, (1\ 2)\}.$$



Solution

 We use Strategy E1. 



The left cosets are as follows.

 The first left coset is H itself. 

$$H = \{e, (1\ 2)\}$$

 Now we choose an element of S_3 not in H , say $(1\ 3)$, and find $(1\ 3)H$. 

$$\begin{aligned} (1\ 3)H &= \{(1\ 3) \circ e, (1\ 3) \circ (1\ 2)\} \\ &= \{(1\ 3), (1\ 2\ 3)\} \end{aligned}$$

 Next we choose an element not in H or $(1\ 3)H$, say $(2\ 3)$, and find $(2\ 3)H$. 

$$\begin{aligned} (2\ 3)H &= \{(2\ 3) \circ e, (2\ 3) \circ (1\ 2)\} \\ &= \{(2\ 3), (1\ 3\ 2)\} \end{aligned}$$

 Every element of S_3 has now been assigned to a left coset. 

So the partition of S_3 into left cosets of H is

$$\{e, (1\ 2)\}, \quad \{(1\ 3), (1\ 2\ 3)\}, \quad \{(2\ 3), (1\ 3\ 2)\}.$$

Exercise E41

Partition the alternating group

$$A_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \\ (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), \\ (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$$

into left cosets of the subgroup

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

(This set H is a subgroup of A_4 because it is a subset of A_4 and its elements represent the symmetries of the rectangle, as you saw in Table 3 in Subsection 1.3.)

Left cosets and their properties can be used to provide a very straightforward proof of Lagrange's Theorem, as follows.

Theorem B68 Lagrange's Theorem

Let G be a finite group and let H be any subgroup of G . Then the order of H divides the order of G .

Proof Let G and H have orders n and m , respectively, and let the number of left cosets of H in G be k . Each left coset has m elements, and the left cosets form a partition of G , so the total number of elements in G is km . That is, $n = km$. Hence m divides n . ■

Although all the examples of left cosets that you have met in this subsection are left cosets in *finite* groups, the definition of left coset applies to any group, whether it is finite or infinite. All the properties of left cosets that we have obtained, and the proofs of these properties, apply to infinite groups as well as to finite ones, unless stated otherwise. In particular, the left cosets of a subgroup of an infinite group form a partition of the group.

A subgroup of an infinite group may have infinitely many distinct left cosets, or only finitely many: you will meet examples of the second possibility in Subsection 4.3, and an example of the first possibility in the next unit.



Frank Nelson Cole

The term ‘coset’ was first introduced by the American mathematician George Abram Miller (1863–1951) in 1910. In 1893 Miller had taken up a position at the University of Michigan where he came under the influence of Frank Nelson Cole (1861–1926), and it was Cole who inspired Miller to devote himself to group theory. Cole had been a student of Felix Klein (1849–1925) in Leipzig, and in 1892 published an English translation of the 1882 book on group theory by Eugen Netto (1846–1919). Cole’s translation was the first book on group theory in English and it was important for stimulating interest in the subject.

4.2 Right cosets

In the previous subsection the *left* coset gH of a subgroup H of a group (G, \circ) was defined to be the set

$$gH = \{gh : h \in H\}.$$

That is, it is the subset of G obtained by composing each element of H with g on the *left*.

Right cosets are defined in the same way, but with the composition with g on the right, as below.

Definition

Let H be a subgroup of a group G , and let g be an element of G . The **right coset** Hg of H is given by

$$Hg = \{hg : h \in H\}.$$

It is the subset of G obtained by composing each element of H with g on the right.

For example, consider the subgroup $H = \{e, r\}$ of the group $S(\square)$, and the element $a \in S(\square)$. The right coset Ha of H in $S(\square)$ is

$$Ha = \{e, r\}a = \{e \circ a, r \circ a\} = \{a, u\}.$$

In the previous subsection we found all the left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$. In the next worked exercise we find all the right cosets of the same subgroup.

Worked Exercise E14

Find all the right cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$. (The group table of $S(\square)$ is given as Table 9.)

Solution

For each $g \in S(\square)$, we find the right coset Hg .

$$He = \{e, r\}e = \{e \circ e, r \circ e\} = \{e, r\},$$

$$Ha = \{e, r\}a = \{e \circ a, r \circ a\} = \{a, u\},$$

$$Hb = \{e, r\}b = \{e \circ b, r \circ b\} = \{b, t\},$$

$$Hc = \{e, r\}c = \{e \circ c, r \circ c\} = \{c, s\},$$

$$Hr = \{e, r\}r = \{e \circ r, r \circ r\} = \{r, e\},$$

$$Hs = \{e, r\}s = \{e \circ s, r \circ s\} = \{s, c\},$$

$$Ht = \{e, r\}t = \{e \circ t, r \circ t\} = \{t, b\},$$

$$Hu = \{e, r\}u = \{e \circ u, r \circ u\} = \{u, a\}.$$

Table 9 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

As with left cosets, some of the right cosets found in Worked Exercise E14 turn out to be the same set as each other:

$$He = Hr = \{e, r\},$$

$$Ha = Hu = \{a, u\},$$

$$Hb = Ht = \{b, t\},$$

$$Hc = Hs = \{c, s\}.$$

The *distinct* right cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$ are

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

Notice also that the right coset Ha of $H = \{e, r\}$ is not the same set as the corresponding left coset aH . We found above that

$$Ha = \{e, r\}a = \{e \circ a, r \circ a\} = \{a, u\},$$

whereas we found earlier, in Worked Exercise E11, that

$$aH = a\{e, r\} = \{a \circ e, a \circ r\} = \{a, s\}.$$

So, in general, left cosets and right cosets are different sets.

However, sometimes left and right cosets turn out to be the same set. For example, again for the subgroup $H = \{e, r\}$ of the group $S(\square)$, we found above that

$$Hb = \{e, r\}b = \{e \circ b, r \circ b\} = \{b, t\}$$

and earlier, in Worked Exercise E11, we found that

$$bH = b\{e, r\} = \{b \circ e, b \circ r\} = \{b, t\}.$$

So in this instance $Hb = bH$.

All the results for left cosets that you met in the previous subsection have analogous results for right cosets, as stated below. The proofs of these results are analogues of the proofs for left cosets given earlier, so are omitted here.

Theorem E4

Let H be a subgroup of a group G . Then the distinct right cosets of H in G form a partition of G .

Proposition E5 Properties of right cosets

Let H be a subgroup of a group G .

- (a) The element g lies in the right coset Hg , for each $g \in G$.
- (b) One of the right cosets of H in G is H itself.
- (c) Any two right cosets Hg_1 and Hg_2 are either the same set or are disjoint.
- (d) If H is finite, then each right coset Hg has the same number of elements as H .

We also have the following strategy for finding right cosets in a finite group efficiently, analogous to Strategy E1 for left cosets.

Strategy E2

To partition a finite group G into right cosets of a subgroup H , do the following.

1. Take H as the first right coset.
2. Choose any element $g \in G$ not yet assigned to a right coset and determine the right coset Hg to which g belongs.
3. Repeat step 2 until every element of G has been assigned to a right coset.

This strategy is demonstrated in the next worked exercise, in which the right cosets found in Worked Exercise E14 are found again, but this time more efficiently.

Worked Exercise E15

Partition the group $S(\square)$ into right cosets of the subgroup $H = \{e, r\}$. (The group table of $S(\square)$ is given as Table 10.)

Solution

We use Strategy E2.

The right cosets are as follows.

The first right coset is H itself.

$$H = \{e, r\}$$

Now we choose an element of $S(\square)$ not in H , say a , and find Ha .

$$Ha = \{e \circ a, r \circ a\} = \{a, u\}$$

Next we choose an element not in H or Ha , say b , and find Hb .

$$Hb = \{e \circ b, r \circ b\} = \{b, t\}$$

Now we choose an element not in H , Ha or Hb , say c , and find Hc .

$$Hc = \{e \circ c, r \circ c\} = \{c, s\}$$

Every element has now been assigned to a right coset.

So the partition of $S(\square)$ into right cosets of H is

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

Table 10 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

Exercise E42

Partition $S(\triangle)$ into right cosets of the subgroup $H = \{e, s\}$. (The group table of $S(\triangle)$ is given as Table 11.)

We now have two ways to partition a group into cosets of a subgroup: the partition into left cosets and the partition into right cosets. You have seen that these two partitions may not be the same. For example, in Worked Exercise E12 in the previous subsection we found that the partition of $S(\square)$ into left cosets of the subgroup $\{e, r\}$ is

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\},$$

whereas the partition of $S(\square)$ into right cosets of the same subgroup, which we found in Worked Exercise E15, is

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

Table 11 $S(\triangle)$

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

These two partitions of $S(\square)$ are shown in Figure 26.

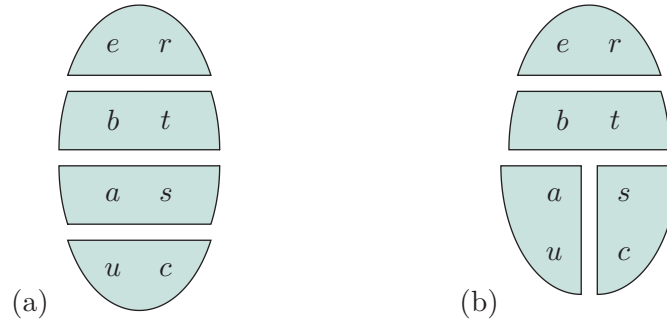


Figure 26 The partitions of $S(\square)$ into (a) left and (b) right cosets of $\{e, r\}$

Similarly, the partition of $S(\triangle)$ into left cosets of its subgroup $\{e, s\}$, which you were asked to find in Exercise E36 in Subsection 4.1, is

$$\{e, s\}, \quad \{a, r\}, \quad \{b, t\},$$

and this is not the same as the partition of $S(\triangle)$ into right cosets of $\{e, s\}$, which you were asked to find in Exercise E42, and which is

$$\{e, s\}, \quad \{a, t\}, \quad \{b, r\}.$$

These two partitions of $S(\triangle)$ are shown in Figure 27.

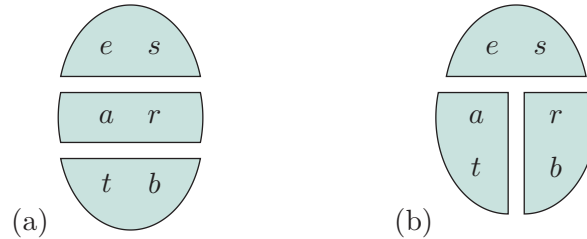


Figure 27 The partitions of $S(\triangle)$ into (a) left and (b) right cosets of $\{e, s\}$

However, sometimes the partitions of a group into left cosets and right cosets of a subgroup are the same. For example, this always happens if the group is abelian. This is because if H is any subgroup of an abelian group G and g is any element of G , then the left coset gH and the right coset Hg are the same set:

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg.$$

The partitions into left cosets and right cosets can also be the same for some groups and subgroups where the group is *non-abelian*. We will consider this possibility in Section 5.

There is in fact a simple connection between the left cosets and the right cosets of a subgroup of a group. If we take the partition into left cosets, and replace every element by its inverse, then we obtain the partition into right cosets, and vice versa.

For example, consider the group $S(\square)$ and its subgroup $\{e, r\}$ again. The partition of $S(\square)$ into left cosets of the subgroup $\{e, r\}$, found in Worked Exercise E12, is

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

Let us replace each element in this partition by its inverse. The elements a and c are inverses of each other, and every other element is self-inverse.

Replacing each element by its inverse gives the following.

$$\begin{array}{cccc} \{e, r\} & \{a, s\} & \{b, t\} & \{c, u\} \\ \downarrow \downarrow & \downarrow \downarrow & \downarrow \downarrow & \downarrow \downarrow \\ \{e, r\} & \{c, s\} & \{b, t\} & \{a, u\} \end{array}$$

The result is the partition of $S(\square)$ into right cosets of the subgroup $\{e, r\}$, which we found in Worked Exercise E15 to be

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

(The order in which the cosets in the partition are listed does not matter, of course.)

This connection between left cosets and right cosets is stated as a theorem below, and you are asked to provide most of the proof as an exercise.

Theorem E6

Let H be a subgroup of a group G .

- (a) If every element in the partition of G into left cosets of H is replaced by its inverse, then the result is the partition of G into right cosets of H .
- (b) The same is true if the words ‘left’ and ‘right’ are interchanged.

Proof We need to prove only part (a). Part (b) then follows immediately, since the inverse of the inverse of an element is the original element.

To prove part (a), we have to prove that every pair of elements x and y of G lie in the same left coset of H if and only if their inverses x^{-1} and y^{-1} lie in the same right coset of H . Now saying that x and y lie in the same left coset of H is the same as saying that $x \in yH$, and similarly saying that x^{-1} and y^{-1} lie in the same right coset of H is the same as saying that $y^{-1} \in Hx^{-1}$. So the fact that we need to prove follows from Exercise E43 below. ■

Exercise E43

Let H be a subgroup of a group G , and let $x, y \in G$. Prove that

$$x \in yH \iff y^{-1} \in Hx^{-1},$$

by proving the \implies part and the \impliedby part separately.

Note that Theorem E6 does *not* say that if H is a subgroup of a group G and g is an element of G then replacing every element of the left coset gH by its inverse gives the right coset Hg . This procedure certainly gives a right coset of H in G , by Theorem E6, but it may not be the right coset Hg .

Theorem E6 has the following immediate corollary.

Corollary E7

Let H be a subgroup of a group G . Then the number of distinct left cosets of H in G is equal to the number of distinct right cosets of H in G (or there may be infinitely many of each).

We can now make the following definition.

Definition

The number of distinct left cosets, or, equivalently, the number of distinct right cosets, of a subgroup H in a group G is called the **index** of H in G .

If H has infinitely many left cosets, or, equivalently, infinitely many right cosets, in G , then we say that H has **infinite index** in G .

For example, you saw earlier that the subgroup $H = \{e, r\}$ of the group $S(\square)$ has four left cosets in $S(\square)$ (and also four right cosets), so the index of the subgroup $H = \{e, r\}$ in $S(\square)$ is 4.

It is straightforward to work out the index of a subgroup H in a *finite* group G , as follows. (Remember that we use the notation $|G|$ for the order of a finite group G .)

Proposition E8

Let H be a subgroup of a finite group G . Then the index of H in G is $|G|/|H|$.

Proof This holds because the left cosets (or right cosets) of H partition G and each left coset (and each right coset) has $|H|$ elements. ■

If H is a subgroup of an *infinite* group G , then H may have infinitely many left cosets (and hence infinitely many right cosets) in G , or only finitely many. That is, H may have infinite index in G , or finite index. You will see examples of the second possibility in the next subsection, and examples of the first possibility in the next unit.

4.3 Cosets in additive groups

In this subsection we consider cosets in additive groups. Examples of additive groups include $(\mathbb{Z}, +)$ and $(\mathbb{Z}_9, +_9)$.

Since all additive groups are abelian, the left cosets of any subgroup of an additive group are the same as the right cosets. So there is no need to distinguish between left and right cosets, and we refer simply to *cosets*.

For an additive group, we denote cosets using notation of the form $g + H$ rather than gH , as follows.

Convention

Let H be a subgroup of an additive group $(G, +)$, and let g be an element of G . The coset $g + H$ of H is the set

$$g + H = \{g + h : h \in H\}.$$

Worked Exercise E16

Partition the group \mathbb{Z}_9 into cosets of the subgroup $H = \langle 3 \rangle = \{0, 3, 6\}$.


Solution

 We use Strategy E1 for partitioning a group into cosets of a subgroup. 



The cosets are as follows.

 The first coset is H itself. 


$$H = \{0, 3, 6\}$$

 Now we choose an element not in H , say 1, and find $1 + H$. 

$$1 + H = \{1 +_9 0, 1 +_9 3, 1 +_9 6\} = \{1, 4, 7\}$$

 Next we choose an element not in H or $1 + H$, say 2, and find $2 + H$. 

$$2 + H = \{2 +_9 0, 2 +_9 3, 2 +_9 6\} = \{2, 5, 8\}$$

 Every element has now been assigned to a coset. 

The partition of \mathbb{Z}_9 into cosets of H is therefore

$$\{0, 3, 6\}, \quad \{1, 4, 7\}, \quad \{2, 5, 8\}.$$

Exercise E44

In each of parts (a) and (b) below, partition the group \mathbb{Z}_{10} into cosets of the subgroup H .

(a) $H = \langle 2 \rangle = \{0, 2, 4, 6, 8\}$ (b) $H = \langle 5 \rangle = \{0, 5\}$

Next we look briefly at some examples of partitioning an *infinite* group into cosets of a subgroup. Remember that a subgroup of an infinite group can have infinitely many cosets in the group, or only finitely many: that is, it can have either infinite index or finite index in the group.

If a subgroup has infinite index, then although we could use our usual strategy for finding cosets, Strategy E1, to find more and more of them, we would never find them all. However, if it has finite index, then we can use the strategy to find all the cosets.

In the next worked exercise we use Strategy E1 to partition an infinite additive group into cosets of a subgroup that has finite index.

Worked Exercise E17



Explain how you know that the set

$$H = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

is a subgroup of the group $(\mathbb{Z}, +)$, and partition \mathbb{Z} into cosets of H .

Solution

The set H is the cyclic subgroup of $(\mathbb{Z}, +)$ generated by 3, so it is a subgroup of $(\mathbb{Z}, +)$.

 To find its cosets in $(\mathbb{Z}, +)$, we use Strategy E1. 



The cosets are as follows.

 The first coset is H itself. 

$$H = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

 We then choose an element not in H , say 1, and find $1 + H$. 

$$\begin{aligned} 1 + H &= \{\dots, -6, -3, 0, 3, 6, \dots\} \\ &= \{\dots, 1 + (-6), 1 + (-3), 1 + 0, 1 + 3, 1 + 6, \dots\} \\ &= \{\dots, -5, -2, 1, 4, 7, \dots\} \end{aligned}$$

 Next we choose an element not in H or $1 + H$, say 2, and find $2 + H$. 

$$\begin{aligned} 2 + H &= \{\dots, -6, -3, 0, 3, 6, \dots\} \\ &= \{\dots, 2 + (-6), 2 + (-3), 2 + 0, 2 + 3, 2 + 6, \dots\} \\ &= \{\dots, -4, -1, 2, 5, 8, \dots\} \end{aligned}$$

☁ Every element has now been assigned to a coset. ☁

The partition of $(\mathbb{Z}, +)$ into cosets of H is therefore

$$\begin{aligned} H &= \{\dots, -6, -3, 0, 3, 6, \dots\}, \\ 1 + H &= \{\dots, -5, -2, 1, 4, 7, \dots\}, \\ 2 + H &= \{\dots, -4, -1, 2, 5, 8, \dots\}. \end{aligned}$$

The subgroup H in Worked Exercise E17 is the subset of \mathbb{Z} that we denoted by $3\mathbb{Z}$ in Exercise E33:

$$3\mathbb{Z} = \{3k : k \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}.$$

In general, for any number x , we denote the set of integer multiples of x by $x\mathbb{Z}$; that is,

$$x\mathbb{Z} = \{xk : k \in \mathbb{Z}\} = \{\dots, -2x, -x, 0, x, 2x, 3x, \dots\}.$$

For any *integer* n , the set

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

is a subgroup of $(\mathbb{Z}, +)$, because it is the cyclic subgroup of $(\mathbb{Z}, +)$ generated by n .

Exercise E45

- (a) Partition the group $(\mathbb{Z}, +)$ into cosets of the subgroup $4\mathbb{Z}$.
- (b) Partition the group $(2\mathbb{Z}, +)$ into cosets of the subgroup $6\mathbb{Z}$.

The blue box below expands on the blue box *Permutations and bell ringing* in Subsection 2.4 of Unit B3. If you want to read it, you may find it helpful to read the earlier box again first. Remember that all the material in the blue boxes is optional.

Cosets and bell ringing

The blue box *Permutations and bell ringing* in Unit B3 explained that church bell ringers usually ring a sequence of bells in which each bell rings exactly once, then another such sequence with the bells in a different order, then another, and so on, until they have rung a number of such sequences, all different, in some sort of pattern. The order of the sequences in the pattern must be such that each bell changes by at most one place from each sequence to the next.

For example, the table below, repeated from Unit B3, shows a suitable pattern for ringing sequences of four bells A , B , C and D .



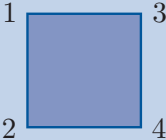
Bells in the Church of the Assumption of the Blessed Virgin Mary, Leckhampstead, Buckinghamshire



Bell ringers at the Church of the Assumption of the Blessed Virgin Mary, Lillingstone Lovell, Buckinghamshire

The coloured lines trace the changes in place of each bell. The eight sequences of bells are all different, and each bell changes by at most one place from each sequence to the next.

| Sequence of bells | Permutation applied | Permutation from start |
|-----------------------------|---------------------|------------------------|
| $A \quad B \quad C \quad D$ | | e |
| $B \quad A \quad D \quad C$ | $(1 \ 2)(3 \ 4)$ | $(1 \ 2)(3 \ 4)$ |
| $B \quad D \quad A \quad C$ | $(2 \ 3)$ | $(1 \ 3 \ 4 \ 2)$ |
| $D \quad B \quad C \quad A$ | $(1 \ 2)(3 \ 4)$ | $(1 \ 4)$ |
| $D \quad C \quad B \quad A$ | $(2 \ 3)$ | $(1 \ 4)(2 \ 3)$ |
| $C \quad D \quad A \quad B$ | $(1 \ 2)(3 \ 4)$ | $(1 \ 3)(2 \ 4)$ |
| $C \quad A \quad D \quad B$ | $(2 \ 3)$ | $(1 \ 2 \ 4 \ 3)$ |
| $A \quad C \quad B \quad D$ | $(1 \ 2)(3 \ 4)$ | $(2 \ 3)$ |



The column headed ‘Permutation applied’ in the table shows the permutation of places that is applied to obtain each sequence of bells from the one before. For example, the second sequence $BADC$ is obtained from the first sequence $ABCD$ by interchanging the bells in places 1 and 2 and interchanging the bells in places 3 and 4, that is, by applying the transposition $(1 \ 2)(3 \ 4)$.

The column headed ‘Permutation from start’ shows the permutation of places that is applied to obtain each sequence from the *first* sequence. For example, since the second sequence is obtained from the first sequence by applying $(1 \ 2)(3 \ 4)$, and the third sequence is obtained from the second sequence by applying $(2 \ 3)$, it follows that the third sequence is obtained from the first sequence by applying

$$(2 \ 3) \circ (1 \ 2)(3 \ 4) = (1 \ 3 \ 4 \ 2).$$

Similarly, the fourth sequence is obtained from the first sequence by applying

$$(1 \ 2)(3 \ 4) \circ (1 \ 3 \ 4 \ 2) = (1 \ 4),$$

and so on.

Since two sequences of bells are different if and only if the permutations of places applied to obtain them from the first sequence are different, the eight permutations in the ‘Permutation from start’ column are all different. In fact these eight permutations are the elements of the group $S(\square)$, when the square is labelled as shown on the right above.

A pattern for ringing n bells that contains all possible sequences of the n bells is known as an *extent* for n bells. The pattern in the table above is only a partial extent for four bells, because it contains only

eight sequences whereas the total number of possible sequences for four bells is $4! = 24$. The pattern cannot be extended to a full extent for four bells by continuing it in the same way, that is, by applying the permutations of places $(1\ 2)(3\ 4)$ and $(2\ 3)$ alternately to each new sequence of bells, because applying the permutation $(2\ 3)$ to the eighth sequence gives the first sequence again.

However, the partial extent in the table can be extended to a full extent for four bells by using the idea of *cosets*. Let H be the subgroup of S_4 (isomorphic to $S(\square)$) whose elements appear in the ‘Permutation from start’ column of the table. Each element of H corresponds to a different sequence of bells, as explained above. To extend the partial extent, we disrupt the pattern by applying the transposition $(3\ 4)$ instead of $(2\ 3)$ to the eighth sequence of bells, as shown in the table below. Since the eighth sequence of bells corresponds to the permutation $(2\ 3)$, the ninth sequence of bells then corresponds to the permutation

$$(3\ 4) \circ (2\ 3) = (2\ 4\ 3).$$

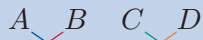


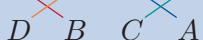

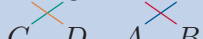

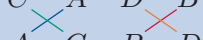
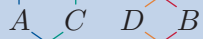


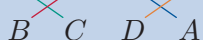

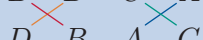

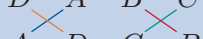



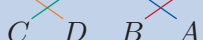

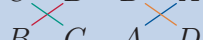

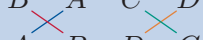
This is not in H , so the ninth sequence of bells is different from the first eight sequences. We then continue the pattern in the same way as before, by applying the permutations of places $(1\ 2)(3\ 4)$ and $(2\ 3)$ alternately: a little thought shows that this amounts to composing each of the elements of H in turn on the right by the permutation $(2\ 4\ 3)$, as shown in the table below. So we obtain the eight sequences of bells corresponding to the eight elements of the right coset $H(2\ 4\ 3)$ of H in S_4 .

We then disrupt the pattern a second time by again applying the transposition $(3\ 4)$. Since the sixteenth sequence of bells corresponds to the permutation $(2\ 3) \circ (2\ 4\ 3)$, the seventeenth sequence of bells then corresponds to the permutation

$$(3\ 4) \circ (2\ 3) \circ (2\ 4\ 3) = (2\ 3\ 4).$$

This is not in H or $H(2\ 4\ 3)$, so the seventeenth sequence of bells is different from the first sixteen sequences. We then continue the pattern in the same way as before, which amounts to composing each of the elements of H in turn on the right by the permutation $(2\ 3\ 4)$, as shown in the table. So we obtain the eight sequences of bells corresponding to the eight elements of the third and final right coset $H(2\ 3\ 4)$ of H in S_4 .

Since the right cosets of H partition S_4 , in this way we obtain all 24 different permutations in S_4 , corresponding to the 24 different sequences of four bells. Notice that applying the ‘disrupting’ permutation $(3\ 4)$ to the final sequence gives the first sequence again, so bell ringers can ring the extent in the table several times consecutively if they wish.

| Sequence of bells | Permutation applied | Permutation from start | |
|---|------------------------|--------------------------------|--------------|
|  | | e | H |
|  | $(1\ 2)(3\ 4)$ | $(1\ 2)(3\ 4)$ | |
|  | $(2\ 3)$ | $(1\ 3\ 4\ 2)$ | |
|  | $(1\ 2)(3\ 4)$ | $(1\ 4)$ | |
|  | $(2\ 3)$ | $(1\ 4)(2\ 3)$ | |
|  | $(1\ 2)(3\ 4)$ | $(1\ 3)(2\ 4)$ | |
|  | $(2\ 3)$ | $(1\ 2\ 4\ 3)$ | |
|  | $(1\ 2)(3\ 4)$ | $(2\ 3)$ | |
| <hr/> | | | |
|  | $(3\ 4)$ | $(2\ 4\ 3)$ | $H(2\ 4\ 3)$ |
|  | $(1\ 2)(3\ 4)$ | $(1\ 2)(3\ 4) \circ (2\ 4\ 3)$ | |
|  | $(2\ 3)$ | $(1\ 3\ 4\ 2) \circ (2\ 4\ 3)$ | |
|  | $(1\ 2)(3\ 4)$ | $(1\ 4) \circ (2\ 4\ 3)$ | |
|  | $(2\ 3)$ | $(1\ 4)(2\ 3) \circ (2\ 4\ 3)$ | |
|  | $(1\ 2)(3\ 4)$ | $(1\ 3)(2\ 4) \circ (2\ 4\ 3)$ | |
|  | $(2\ 3)$ | $(1\ 2\ 4\ 3) \circ (2\ 4\ 3)$ | |
|  | $(1\ 2)(3\ 4)$ | $(2\ 3) \circ (2\ 4\ 3)$ | |
| <hr/> | | | |
|  | $(3\ 4)$ | $(2\ 3\ 4)$ | $H(2\ 3\ 4)$ |
|  | $(1\ 2)(3\ 4)$ | $(1\ 2)(3\ 4) \circ (2\ 3\ 4)$ | |
|  | $(2\ 3)$ | $(1\ 3\ 4\ 2) \circ (2\ 3\ 4)$ | |
|  | $(1\ 2)(3\ 4)$ | $(1\ 4) \circ (2\ 3\ 4)$ | |
|  | $(2\ 3)$ | $(1\ 4)(2\ 3) \circ (2\ 3\ 4)$ | |
|  | $(1\ 2)(3\ 4)$ | $(1\ 3)(2\ 4) \circ (2\ 3\ 4)$ | |
|  | $(2\ 3)$ | $(1\ 2\ 4\ 3) \circ (2\ 3\ 4)$ | |
|  | $(1\ 2)(3\ 4)$ | $(2\ 3) \circ (2\ 3\ 4)$ | |

The pattern of eight sequences of four bells in the first table in this blue box is known to bell ringers as *plain hunt minimus*, and the pattern of 24 sequences in the second table is known as *plain bob minimus*. The word ‘minimus’ indicates that the pattern is rung on four bells.

5 Normal subgroups

In the previous section you saw that the partition of a group into left cosets of a particular subgroup may be different from its partition into right cosets of the same subgroup. You saw that if the group is abelian then the two partitions are the same.

There are also some *non-abelian* groups and subgroups for which the two partitions are the same, as illustrated by the following worked exercise.

Worked Exercise E18

Show that the partition of $S(\square)$ into left cosets of the subgroup $H = \{e, b\}$ is the same as its partition into right cosets of this subgroup. (The group table of $S(\square)$ is given as Table 12.)

Solution

First we find the partition into left cosets, using Strategy E1.

The left cosets are as follows.

$$H = \{e, b\}$$

$$aH = \{a \circ e, a \circ b\} = \{a, c\}$$

$$rH = \{r \circ e, r \circ b\} = \{r, t\}$$

$$sH = \{s \circ e, s \circ b\} = \{s, u\}$$

So the partition into left cosets is

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

To find the partition into right cosets, we could use Strategy E2, the right coset analogue of Strategy E1. However, it is quicker to use Theorem E6: to obtain the partition into right cosets we replace each element in the partition into left cosets by its inverse.

In $S(\square)$ the elements a and c are inverses of each other and all the other elements are self-inverse. So the partition into right cosets is

$$\{e, b\}, \quad \{c, a\}, \quad \{r, t\}, \quad \{s, u\},$$

that is,

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

Thus the partitions into left cosets and right cosets are the same.

Table 12 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

We make the following definition.

Definition

Let G be a group and let H be a subgroup of G . Then H is a **normal subgroup** of G if the partition of G into left cosets of H is the same as the partition of G into right cosets of H . We also say that H is **normal in G** .

For example, Worked Exercise E18 shows that $\{e, b\}$ is a normal subgroup of $S(\square)$.

On the other hand, the subgroup $\{e, r\}$ of $S(\square)$ is *not* a normal subgroup of $S(\square)$, because, as you saw in Worked Exercises E12 and E15, for this subgroup the partitions into left cosets and right cosets are different.

Normal subgroups play an important role in group theory, as you will see throughout the rest of this book. Some texts use the notation $H \triangleleft G$ to assert that H is a normal subgroup of G , but we will not use this notation in this module.

Exercise E46

Determine whether each of the following subgroups of $S(\triangle)$ is normal.

- (a) $\langle t \rangle = \{e, t\}$ (b) $S^+(\triangle) = \{e, a, b\}$ (c) $\{e\}$ (d) $S(\triangle)$

(The group table of $S(\triangle)$ is given as Table 13. In Exercise E40 in Subsection 4.1 you were asked to partition $S(\triangle)$ into left cosets of the subgroup $\langle t \rangle = \{e, t\}$.)

Table 13 $S(\triangle)$

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

Exercise E47

Consider the alternating group

$$A_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \\ (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), \\ (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}.$$

- (a) Let H be the subgroup $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ of A_4 (it is the cyclic subgroup generated by $(1\ 2\ 3)$).

By finding the left coset $(1\ 2)(3\ 4)H$ and right coset $H(1\ 2)(3\ 4)$, show that H is not a normal subgroup of A_4 .

- (b) Let K be the subgroup $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ of A_4 . (It is the subgroup of S_4 that represents the symmetries of the rectangle when its vertices are labelled 1, 2, 3 and 4.)

Show that K is a normal subgroup of A_4 .

(You were asked to partition A_4 into left cosets of this subgroup in Exercise E41 in Subsection 4.1.)

As illustrated by Exercise E46(c) and (d), every group has at least two normal subgroups, as follows.

Theorem E9

The following are normal subgroups of any group G .

- (a) The trivial subgroup $\{e\}$.
- (b) The whole group G .

Proof Let G be any group.

- (a) Every left coset and every right coset of $\{e\}$ in G contains just one element. So the partition of G into left cosets of $\{e\}$ is the same as the partition of G into right cosets of $\{e\}$. That is, $\{e\}$ is a normal subgroup of G .
- (b) There is only one left coset of G in G , namely G itself, and similarly there is only one right coset of G in G , namely G itself. Thus the partition of G into left cosets of G is the same as the partition of G into right cosets of G . That is, G is a normal subgroup of G . ■

For some groups, the subgroups in Theorem E9 are its *only* normal subgroups. At the other extreme, there are groups in which *every* subgroup is normal. For example, this is the case for every abelian group, as you saw in Subsection 4.2. This is stated and proved formally below.

Theorem E10

In an abelian group, every subgroup is normal.

Proof Let H be any subgroup of an abelian group G , and let g be any element of G . Then the left coset gH and the right coset Hg are the same set:

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg.$$

Thus the partitions of G into left cosets and right cosets of H are the same. Hence H is normal in G . ■

There is another straightforward situation in which a subgroup of a group is guaranteed to be a normal subgroup. This is when the subgroup has exactly two left cosets, or, equivalently, exactly two right cosets. This was the case in Exercise E46(b), for example, in which you saw that $S^+(\triangle) = \{e, a, b\}$ is a normal subgroup of $S(\triangle)$ because the partitions into left cosets and right cosets are both as follows:

$$\{e, a, b\}, \quad \{r, s, t\}.$$

The general result is stated as the next theorem, using the term *index*. Remember that the index of a subgroup in a group is the number of left cosets, or, equivalently, the number of right cosets, that it has in the group. The number of left cosets is always equal to the number of right cosets by Corollary E7.

Theorem E11

Every subgroup of index 2 in a group is a normal subgroup of the group.

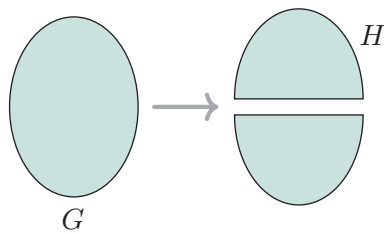


Figure 28 A group G partitioned into two cosets of a subgroup H

Proof Let H be a subgroup of index 2 in a group G ; that is, H has exactly two left cosets and exactly two right cosets in G . Then the partition of G into left cosets of H and the partition of G into right cosets of H must each consist of the subgroup itself and a second coset containing all the elements of G that are not in H , as illustrated in Figure 28. Thus the two partitions are the same, so H is a normal subgroup of G . ■

A subgroup of index 2 in a *finite* group G is simply a subgroup whose order is half of the order of G . However, an infinite group can also have a subgroup of index 2.

The following result about symmetric groups follows from Theorem E11.

Corollary E12

For each positive integer n , the alternating group A_n is a normal subgroup of the symmetric group S_n .

Proof For $n \geq 2$, this follows from the facts that the order of S_n is $n!$ and the order of A_n is $n!/2$. (See Theorems B53 and B62, restated in Subsection 1.2.) For $n = 1$ it follows from the fact that $A_1 = S_1$. ■

Exercise E48

Explain how you know that each of the following subgroups is normal in the stated group.

- The subgroup $4\mathbb{Z}$ of the group $(\mathbb{Z}, +)$.
- The subgroup of direct symmetries of the group $S(\text{tet})$ (the symmetry group of the regular tetrahedron).
- The subgroup of direct symmetries of the group $S(\text{4w})$ (the symmetry group of the 4-windmill).

As you have seen, the condition for a subgroup H of a group G to be a normal subgroup of G is that the partition of G into left cosets of H must be the same as the partition of G into right cosets of H . This condition can be expressed algebraically, as stated in the proposition below.

Proposition E13

Let H be a subgroup of a group G . Then H is normal in G if and only if

$$gH = Hg$$

for each element $g \in G$.

Proof

‘If’ part

Suppose that $gH = Hg$ for each element $g \in G$. It follows immediately that the partitions of G into left cosets and right cosets of H are the same, so H is normal in G .

‘Only if’ part

Suppose that H is normal in G . Let g be any element of G . Then gH is the left coset containing g , and Hg is the right coset containing g . Since H is normal, the partitions of G into left cosets and right cosets of H are the same, so we must have $gH = Hg$. ■

It is important to appreciate that the equation $gH = Hg$ in Proposition E13 means that the sets gH and Hg *contain the same elements*: it does not mean that $gh = hg$ for all $h \in H$. For example, for the subgroup $H = S^+(\triangle) = \{e, a, b\}$ of $S(\triangle)$, we have

$$rH = \{r \circ e, r \circ a, r \circ b\} = \{r, s, t\},$$

$$Hr = \{e \circ r, a \circ r, b \circ r\} = \{r, t, s\}.$$

These *sets* are the same, so $rH = Hr$, but, for example,

$$r \circ a = s, \quad \text{whereas} \quad a \circ r = t.$$

If N is a normal subgroup of a group G then, since the left cosets of N are the same as the right cosets of N , we can refer simply to the *cosets* of N , in the same way as we do for subgroups of abelian groups. We will do this throughout the remainder of this book whenever we work with cosets of normal subgroups.

Summary

In this unit you revised many of the fundamental ideas of group theory that you met in Book B. You should now be ready to build on them to understand the deeper group theory in this book. You also met a new family of groups, namely the subgroups of the *general linear group of degree 2*, the group of all invertible 2×2 matrices under matrix multiplication. You started your study of more advanced group theory by meeting the ideas of the *left cosets* and the *right cosets* of a subgroup of a group. You saw that the left cosets of a subgroup of a group are subsets of the group that are ‘shifts’ of the subgroup and that they partition the group, and you saw that the right cosets of the subgroup are similar. You met *normal subgroups*, subgroups for which the partition into left cosets is the same as the partition into right cosets.

Starting in the next unit, you will see how the ideas of cosets and normal subgroups lead us to the concept of *quotient groups*, which is a powerful tool for gaining a deeper understanding of the structures of groups.

Learning outcomes

After working through this unit, you should be able to:

- work fluently with the ideas and techniques from Book B revised in this unit
- determine whether a given set of 2×2 matrices forms a group under matrix multiplication
- determine the *left cosets* and the *right cosets* of a subgroup in a group
- understand that the left cosets and the right cosets of a subgroup in a group each form a *partition* of the group, and determine such partitions
- determine whether a subgroup of a group is a *normal* subgroup of the group.

Solutions to exercises

Solution to Exercise E1

(a) We check the group axioms for $(A, +)$.

G1 Let $g, h \in A$. Then $g = 5m$ and $h = 5n$ for some integers m, n . Hence

$$g + h = 5m + 5n = 5(m + n).$$

Since $m + n$ is an integer, this shows that $g + h \in A$. Thus A is closed under addition.

G2 Addition of integers is associative.

G3 We have $0 \in A$, and for all $g \in A$,

$$g + 0 = g = 0 + g.$$

So 0 is an identity element for $+$ on A .

G4 Let $g \in A$. Then $g = 5m$ for some integer m . Now

$$-g = -(5m) = 5(-m).$$

Since $-m$ is an integer, this shows that $-g \in A$. Also

$$g + (-g) = 0 = -g + g.$$

Thus each element of A has an inverse in A with respect to addition.

Hence $(A, +)$ satisfies the four group axioms, and so is a group.

(b) We check the group axioms for (A, \times) .

G1 Let $g, h \in A$. Then $g = 5m$ and $h = 5n$ for some integers m, n . Hence

$$g \times h = 5m \times 5n = 5(5mn).$$

Since $5mn$ is an integer, this shows that $g \times h \in A$. Thus A is closed under multiplication.

G2 Multiplication of integers is associative.

G3 Since $1 \notin A$, there is no element $e \in A$ such that

$$g \times e = g = e \times g$$

for all $g \in A$. So there is no identity element for \times on A .

Hence (A, \times) does not satisfy axiom G3, so it is not a group.

(It is not necessary to confirm that axioms G1 and G2 are satisfied here: you can just show that axiom G3 is not satisfied.)

Solution to Exercise E2

We check the group axioms for $([0, 1), +_1)$.

G1 Let $x, y \in [0, 1)$. By the definition of the binary operation $+_1$,

$$x +_1 y \in [0, 1).$$

Thus $[0, 1)$ is closed under $+_1$.

G2 We are given that $+_1$ is associative on $[0, 1)$.

G3 We have $0 \in [0, 1)$, and for all $x \in [0, 1)$,

$$\begin{aligned} x +_1 0 &= \text{frac}(x + 0) \\ &= \text{frac}(x) \\ &= x \quad (\text{since } x \in [0, 1)), \end{aligned}$$

and similarly

$$0 +_1 x = x.$$

Thus 0 is an identity element for $+_1$ on $[0, 1)$.

G4 The element 0 of $[0, 1)$ has inverse 0 with respect to $+_1$, since

$$0 +_1 0 = 0.$$

Now let x be any other element of $[0, 1)$. Then $1 - x \in [0, 1)$ and we have

$$\begin{aligned} x +_1 (1 - x) &= \text{frac}(x + (1 - x)) \\ &= \text{frac}(1) \\ &= 0, \end{aligned}$$

and similarly

$$(1 - x) +_1 x = 0.$$

Hence $1 - x$ is an inverse of x with respect to $+_1$.

Thus each element of $[0, 1)$ has an inverse in $[0, 1)$ with respect to $+_1$.

Therefore $([0, 1), +_1)$ satisfies the four group axioms, and so is a group.

(Proving that $+_1$ is associative on $[0, 1)$ is trickier than checking the other three group axioms for $([0, 1), +_1)$, but it can be done as follows.

Unit E1 Cosets and normal subgroups

G2 By the definition of $+_1$, if x and y are any elements of $[0, 1)$ then

$$\begin{aligned} x +_1 y &= \text{frac}(x + y) \\ &= x + y - \lfloor x + y \rfloor, \end{aligned}$$

so $x +_1 y$ is equal to $x + y$ minus some integer.

Now let $x, y, z \in [0, 1)$. Then

$$\begin{aligned} (x +_1 y) +_1 z &= (x + y - p) +_1 z \quad \text{where } p \in \mathbb{Z} \\ &= (x + y - p) + z - q \quad \text{where } q \in \mathbb{Z} \\ &= x + y + z - (p + q). \end{aligned}$$

Similarly,

$$\begin{aligned} x +_1 (y +_1 z) &= x +_1 (y + z - r) \quad \text{where } r \in \mathbb{Z} \\ &= x + (y + z - r) - s \quad \text{where } s \in \mathbb{Z} \\ &= x + y + z - (r + s). \end{aligned}$$

Since $(x +_1 y) +_1 z$ and $x +_1 (y +_1 z)$ both lie in the interval $[0, 1)$, the integers $p + q$ and $r + s$ in the final lines of the two manipulations above must be the *same* integer. Therefore

$$(x +_1 y) +_1 z = x +_1 (y +_1 z).$$

Thus $+_1$ is associative on $[0, 1)$.

Solution to Exercise E3

We construct the Cayley table for (G, \times) by multiplying each pair of the matrices **I**, **R**, **S**, **T** individually. The table is as follows.

| \times | I | R | S | T |
|----------|----------|----------|----------|----------|
| I | I | R | S | T |
| R | R | I | T | S |
| S | S | T | I | R |
| T | T | S | R | I |

We consider each axiom in turn.

G1 Every element in the body of the table is in G , so G is closed under matrix multiplication.

G2 Matrix multiplication is associative.

G3 The table shows that the matrix **I** is an identity element for (G, \times) .

G4 The table shows that all the matrices in G are self-inverse.

Since all four axioms hold, (G, \times) is a group.

The Cayley table is symmetric with respect to the main diagonal, so (G, \times) is an abelian group.

Solution to Exercise E4

(a) A Cayley table for $(\{0, 1, 2\}, +_3)$ is as follows.

| $+_3$ | 0 | 1 | 2 |
|-------|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

We consider each axiom in turn.

G1 Every element in the body of the table is in $\{0, 1, 2\}$, so $\{0, 1, 2\}$ is closed under $+_3$.

G2 Modular addition is associative.

G3 The table shows that 0 is an identity element for $+_3$ on $\{0, 1, 2\}$.

G4 The table shows that 0 is self-inverse, and 1 and 2 are inverses of each other.

Since all four axioms hold, $(\{0, 1, 2\}, +_3)$ is a group.

(b) A Cayley table for $(\{2, 4, 6\}, \times_8)$ is as follows.

| \times_8 | 2 | 4 | 6 |
|------------|---|---|---|
| 2 | 4 | 0 | 4 |
| 4 | 0 | 0 | 0 |
| 6 | 4 | 0 | 4 |

The integer 0 appears in the body of the table, but $0 \notin \{2, 4, 6\}$, so $\{2, 4, 6\}$ is not closed under \times_8 .

Thus axiom G1 (closure) does not hold, so $(\{2, 4, 6\}, \times_8)$ is not a group.

(c) A Cayley table for $(\{1, 5\}, \times_6)$ is as follows.

| \times_6 | 1 | 5 |
|------------|---|---|
| 1 | 1 | 5 |
| 5 | 5 | 1 |

We consider each axiom in turn.

G1 Every element in the body of the table is in $\{1, 5\}$, so $\{1, 5\}$ is closed under \times_6 .

G2 Modular multiplication is associative.

G3 The table shows that 1 is an identity element for \times_6 on $\{1, 5\}$.

G4 The table shows that 1 and 5 are both self-inverse.

Since all four axioms hold, $(\{1, 5\}, \times_6)$ is a group.

(d) A Cayley table for $(\{3, 9, 15, 21\}, \times_{24})$ is as follows.

| \times_{24} | 3 | 9 | 15 | 21 |
|---------------|----|----|----|----|
| 3 | 9 | 3 | 21 | 15 |
| 9 | 3 | 9 | 15 | 21 |
| 15 | 21 | 15 | 9 | 3 |
| 21 | 15 | 21 | 3 | 9 |

We consider each axiom in turn.

G1 Every element in the body of the table is in $\{3, 9, 15, 21\}$, so $\{3, 9, 15, 21\}$ is closed under \times_{24} .

G2 Modular multiplication is associative.

G3 The table shows that 9 is an identity element for \times_{24} on $\{3, 9, 15, 21\}$.

G4 The table shows that all four elements of $(\{3, 9, 15, 21\}, \times_{24})$ are self-inverse.

Since all four axioms hold, $(\{3, 9, 15, 21\}, \times_{24})$ is a group.

Solution to Exercise E5

(a) $U_{18} = \{1, 5, 7, 11, 13, 17\}$

(b) $U_7 = \{1, 2, 3, 4, 5, 6\}$

(c) $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} = U_7$

Solution to Exercise E6

(a) $(1\ 2\ 7\ 5)(3\ 8\ 4) \circ (1\ 3\ 6\ 7\ 5)$
 $= (1\ 8\ 4\ 3\ 6\ 5\ 2\ 7)$

(b) $(1\ 3\ 7)(2\ 5\ 4) \circ (2\ 4)(3\ 8)(5\ 6)$
 $= (1\ 3\ 8\ 7)(2)(4\ 5\ 6)$
 $= (1\ 3\ 8\ 7)(4\ 5\ 6)$

Solution to Exercise E7

$(1\ 4\ 5\ 6) \circ (2\ 3\ 7\ 4\ 8) \circ (1\ 7\ 6)(3\ 2\ 5)$
 $= (1\ 5\ 7)(2\ 6\ 4\ 8)(3)$
 $= (1\ 5\ 7)(2\ 6\ 4\ 8)$

Solution to Exercise E8

(a) $((1\ 7\ 5\ 2)(3\ 8\ 4))^{-1}$
 $= (2\ 5\ 7\ 1)(4\ 8\ 3)$
 $= (1\ 2\ 5\ 7)(3\ 4\ 8)$ (more usual form)

(b) $((1\ 4)(2\ 3)(6\ 8))^{-1}$
 $= (4\ 1)(3\ 2)(8\ 6)$
 $= (1\ 4)(2\ 3)(6\ 8)$ (more usual form)

(In general, a permutation that contains only cycles of lengths 2 or 1 is self-inverse.)

Solution to Exercise E9

$(1\ 5\ 3)(2\ 4\ 7\ 9\ 6)$
 $= (1\ 3) \circ (1\ 5) \circ (2\ 6) \circ (2\ 9) \circ (2\ 7) \circ (2\ 4)$

Solution to Exercise E10

(a) The parity of $(1\ 5\ 8)(2\ 7\ 3\ 4)$ is
 even + odd = odd.

(b) The parity of $(1\ 8)(2\ 7)(3\ 5\ 4\ 6)$ is
 odd + odd + odd = odd.

Solution to Exercise E11

(a) $a \circ s = r$

(b) $b^{-1} = a$

(We look along the row labelled b until we find e , then note that it is in the column labelled a .)

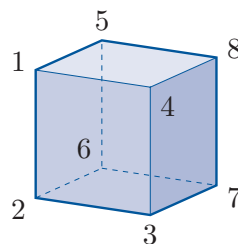
(c) Working from the right, we obtain

$$b \circ r \circ a = b \circ (r \circ a) = b \circ s = t.$$

Alternatively, working from the left, we obtain

$$b \circ r \circ a = (b \circ r) \circ a = s \circ a = t.$$

Solution to Exercise E12



(a) (i) The permutation $(1\ 8)(2\ 7)$ represents the reflection of the cube in the plane 3456.

(ii) The permutation $(1\ 4\ 8\ 5)(2\ 3\ 7\ 6)$ represents a rotation of the cube through $\pi/2$ about the vertical axis of symmetry of the cube. The rotation is anticlockwise when we look down this axis of symmetry from above.

(b) We have

$$(1\ 8)(2\ 7) \circ (1\ 4\ 8\ 5)(2\ 3\ 7\ 6) \\ = (1\ 4)(2\ 3)(5\ 8)(6\ 7)$$

and

$$(1\ 4\ 8\ 5)(2\ 3\ 7\ 6) \circ (1\ 8)(2\ 7) \\ = (1\ 5)(2\ 6)(3\ 7)(4\ 8).$$

The first of these permutations is the reflection in the plane that bisects the edges 14, 23, 58 and 67. The second is the reflection in the plane that bisects the edges 15, 26, 37 and 48.

(c) (i) The rotation through π about the line through the midpoints of the faces 1265 and 4378 is represented by $(1\ 6)(2\ 5)(3\ 8)(4\ 7)$.

(ii) The two non-trivial rotations about the line through the vertices 1 and 7 are represented by $(2\ 4\ 5)(3\ 8\ 6)$ and $(2\ 5\ 4)(3\ 6\ 8)$.

Solution to Exercise E13

(a) The integers 5, 10, 15 and 20 are not coprime to 25, so the set A is not a subset of U_{25} and hence it is not a subgroup of the group (U_{25}, \times_{25}) .

(b) We have $B = \{1, 6, 11, 16, 21\} \subseteq U_{25}$, and the binary operation \times_{25} is the same on each set.

The Cayley table for (B, \times_{25}) is as follows.

| \times_{25} | 1 | 6 | 11 | 16 | 21 |
|---------------|----|----|----|----|----|
| 1 | 1 | 6 | 11 | 16 | 21 |
| 6 | 6 | 11 | 16 | 21 | 1 |
| 11 | 11 | 16 | 21 | 1 | 6 |
| 16 | 16 | 21 | 1 | 6 | 11 |
| 21 | 21 | 1 | 6 | 11 | 16 |

We check the three subgroup properties.

SG1 Every element in the body of the table is in B , so B is closed under \times_{25} .

SG2 The identity element in (U_{25}, \times_{25}) is 1, and we have $1 \in B$.

SG3 The Cayley table shows that the element 1 is self-inverse, the elements 6 and 21 are inverses of each other, and the elements 11 and 16 are inverses of each other. So B contains the inverse of each of its elements.

Hence B satisfies the three subgroup properties and so is a subgroup of (U_{25}, \times_{25}) .

(c) The integers 9 and 11 are in C , but

$$9 \times_{25} 11 = 24 \notin C,$$

so C is not closed under \times_{25} . That is, property SG1 fails.

Hence C is not a subgroup of (U_{25}, \times_{25}) .

Solution to Exercise E14

The set $\{e, x\}$ is a subset of G . Since e is the identity element of (G, \circ) and x is self-inverse, the Cayley table for $(\{e, x\}, \circ)$ is as follows.

| \circ | e | x |
|---------|-----|-----|
| e | e | x |
| x | x | e |

We check the three subgroup properties.

SG1 Every element in the body of the table is in $\{e, x\}$, so this set is closed under \circ .

SG2 The identity element in (G, \circ) is e , and we have $e \in \{e, x\}$.

SG3 The elements e and x are both self-inverse, so $\{e, x\}$ contains the inverse of each of its elements.

Hence $\{e, x\}$ satisfies the three subgroup properties and so is a subgroup of (G, \circ) .

Solution to Exercise E15

(a) The subgroup of order 1 is $\{e\}$.

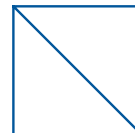
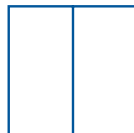
(b) The five subgroups of order 2 are

$$\{e, b\}, \quad \{e, r\}, \quad \{e, s\}, \quad \{e, t\}, \quad \{e, u\}.$$

(c) The three subgroups of order 4 are

$$\{e, a, b, c\}, \quad \{e, b, r, t\}, \quad \{e, b, s, u\}.$$

The first of these is the group of rotations (direct symmetries) of the square; it can be spotted in the top left-hand corner of the group table for $S(\square)$. The subgroups $\{e, b, r, t\}$ and $\{e, b, s, u\}$ can be obtained by considering the symmetries of each of the following modified squares, respectively.



(d) The subgroup of order 8 is $S(\square)$ itself.

Solution to Exercise E16

The subgroup of S_7 obtained from the figure is

$$\{e, (1\ 3\ 7), (1\ 7\ 3), (1\ 3), (1\ 7), (3\ 7)\}.$$

Solution to Exercise E17

(a) We show that the three subgroup properties hold for G .

SG1 Let $f, g \in G$. Then both f and g map each element of A to another element of A . We have to show that $f \circ g$ maps each element of A to another element of A . To do this, let $k \in A$. Then $g(k) \in A$ and hence $f(g(k)) \in A$, that is $(f \circ g)(k) \in A$. Thus $f \circ g$ maps each element of A to another element of A , so $f \circ g \in G$. Thus property SG1 holds.

SG2 The identity permutation e in S_n maps each element of A to itself, so $e \in G$. Thus property SG2 holds.

SG3 Let $f \in G$. Then f maps each element of A to another element of A . We have to show that f^{-1} maps each element of A to another element of A . Since f is one-to-one and maps each element of the finite set A to another element of A , each element of A must occur as the image of an element of A under f . Hence the image of each element of A under f^{-1} is an element of A , as required. Thus property SG3 holds.

Hence G is a subgroup of S_n .

(b) When $n = 5$ and $A = \{4, 5\}$ the elements of the group G defined in part (a) are as follows:

$$\begin{array}{ll} e, & (4\ 5), \\ (1\ 2\ 3), & (1\ 2\ 3)(4\ 5), \\ (1\ 3\ 2), & (1\ 3\ 2)(4\ 5), \\ (1\ 2), & (1\ 2)(4\ 5), \\ (1\ 3), & (1\ 3)(4\ 5), \\ (2\ 3), & (2\ 3)(4\ 5). \end{array}$$

(This group can also be obtained by labelling the vertices of the double tetrahedron: see Worked Exercise B39 in Unit B3.)

Solution to Exercise E18

(a) This matrix has determinant

$$1 \times 2 - 3 \times 0 = 2 - 0 = 2$$

and so is invertible. Its inverse is

$$\frac{1}{2} \begin{pmatrix} 2 & -3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{2} \end{pmatrix}.$$

(b) This matrix is not invertible because it has determinant

$$2 \times (-1) - (-2) \times 1 = -2 + 2 = 0.$$

Solution to Exercise E19

We show that the three subgroup properties hold for D .

SG1 Let $\mathbf{A}, \mathbf{B} \in D$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ 0 & y \end{pmatrix},$$

for some $r, u, v, y \in \mathbb{R}$. Hence

$$\mathbf{AB} = \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix} \begin{pmatrix} v & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} rv & 0 \\ 0 & uy \end{pmatrix}.$$

This is a diagonal matrix, so $\mathbf{AB} \in D$. Thus D is closed under matrix multiplication.

(To show that $\mathbf{AB} \in D$ here we do not need to show that $\mathbf{AB} \in \text{GL}(2)$: we know that already because $\mathbf{A}, \mathbf{B} \in \text{GL}(2)$ and $\text{GL}(2)$ is a group. We just need to show that \mathbf{AB} is diagonal.)

SG2 The identity element $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of $\text{GL}(2)$ is diagonal. Hence $\mathbf{I} \in D$.

SG3 Let $\mathbf{A} \in D$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix},$$

for some $r, u \in \mathbb{R}$. The inverse of \mathbf{A} in $\text{GL}(2)$ is

$$\mathbf{A}^{-1} = \frac{1}{ru} \begin{pmatrix} u & 0 \\ 0 & r \end{pmatrix} = \begin{pmatrix} 1/r & 0 \\ 0 & 1/u \end{pmatrix}.$$

This is a diagonal matrix, so $\mathbf{A}^{-1} \in D$. Thus D contains the inverse of each of its elements.

(To show that $\mathbf{A}^{-1} \in D$ here we do not need to show that $\mathbf{A}^{-1} \in \text{GL}(2)$: we know that already because $\mathbf{A} \in \text{GL}(2)$ and $\text{GL}(2)$ is a group. We just need to show that \mathbf{A}^{-1} is diagonal.)

Since the three subgroup properties hold, D is a subgroup of $\text{GL}(2)$.

(Since every diagonal matrix is also an upper triangular matrix and a lower triangular matrix, it follows that D is also a subgroup of the group L of invertible 2×2 lower triangular matrices, and a subgroup of the group U of invertible 2×2 upper triangular matrices.)

Solution to Exercise E20

We show that the three subgroup properties hold.

SG1 Let $\mathbf{A}, \mathbf{B} \in H$. Then $\det \mathbf{A} = 1$ and $\det \mathbf{B} = 1$. Hence

$$\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B}) = 1 \times 1 = 1.$$

So $\mathbf{AB} \in H$. Thus H is closed under matrix multiplication.

SG2 The identity matrix $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has determinant $1 \times 1 - 0 \times 0 = 1$, so $\mathbf{I} \in H$.

SG3 Let $\mathbf{A} \in H$. Then $\det \mathbf{A} = 1$. Hence

$$\det \mathbf{A}^{-1} = 1/(\det \mathbf{A}) = 1/1 = 1.$$

So $\mathbf{A}^{-1} \in H$. Thus H contains the inverse of each of its elements.

Hence H satisfies the three subgroup properties, so it is a subgroup of $\text{GL}(2)$.

Solution to Exercise E21

(a) The set M is a subset of the group $\text{GL}(2)$, because each matrix

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \quad \text{where } a \neq 0,$$

in M has determinant

$$a \times a - b \times 0 = a^2 \neq 0,$$

and is therefore invertible. Also, the binary operation specified for M is the same as the binary operation of $\text{GL}(2)$. We show that the three subgroup properties hold for M .

SG1 Let $\mathbf{A}, \mathbf{B} \in M$. Then

$$\mathbf{A} = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & w \\ 0 & v \end{pmatrix},$$

for some $r, s, v, w \in \mathbb{R}$ with $r \neq 0$ and $v \neq 0$.

So

$$\mathbf{AB} = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \begin{pmatrix} v & w \\ 0 & v \end{pmatrix} = \begin{pmatrix} rv & rw + sv \\ 0 & rv \end{pmatrix}.$$

This matrix is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = rv$ and $b = rw + sv$. Also, $rv \neq 0$ since $r \neq 0$ and $v \neq 0$. Hence $\mathbf{AB} \in M$. Thus M is closed under matrix multiplication.

SG2 The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of $\text{GL}(2)$ is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = 1$ and $b = 0$. So $\mathbf{I} \in M$.

SG3 Let $\mathbf{A} \in M$. Then

$$\mathbf{A} = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix},$$

for some $r, s \in \mathbb{R}$ with $r \neq 0$. The inverse of \mathbf{A} in $\text{GL}(2)$ is

$$\begin{aligned} \mathbf{A}^{-1} &= \frac{1}{r^2} \begin{pmatrix} r & -s \\ 0 & r \end{pmatrix} \\ &= \begin{pmatrix} 1/r & -s/r^2 \\ 0 & 1/r \end{pmatrix}. \end{aligned}$$

This matrix is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = 1/r$ and $b = -s/r^2$. Also $1/r \neq 0$. Hence $\mathbf{A}^{-1} \in M$. Thus M contains the inverse of each of its elements.

Since the three subgroup properties hold, M is a subgroup of $\text{GL}(2)$. Hence it is a group under matrix multiplication.

(b) The set P is a subset of the group $\text{GL}(2)$, because each matrix

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

in P has determinant

$$a \times \frac{1}{a} - 0 \times 0 = 1,$$

and is therefore invertible. Also, the binary operation specified for P is the same as the binary operation of $\text{GL}(2)$. We show that the three subgroup properties hold for P .

SG1 Let $\mathbf{A}, \mathbf{B} \in P$. Then

$$\mathbf{A} = \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} y & 0 \\ 0 & 1/y \end{pmatrix},$$

for some $x, y \in \mathbb{R}$ with $x \neq 0$ and $y \neq 0$. So

$$\begin{aligned} \mathbf{AB} &= \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1/y \end{pmatrix} \\ &= \begin{pmatrix} xy & 0 \\ 0 & 1/(xy) \end{pmatrix}. \end{aligned}$$

This matrix is of the form

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

with $a = xy$. Also, $xy \neq 0$ since $x \neq 0$ and $y \neq 0$. Hence $\mathbf{AB} \in P$. Thus P is closed under matrix multiplication.

SG2 The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of $\text{GL}(2)$ is in P , since we can write

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1/1 \end{pmatrix},$$

which shows that \mathbf{I} is of the form

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

with $a = 1$.

SG3 Let $\mathbf{A} \in P$. Then

$$\mathbf{A} = \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix},$$

for some $x \in \mathbb{R}$ with $x \neq 0$. The inverse of \mathbf{A} in $\text{GL}(2)$ is

$$\mathbf{A}^{-1} = \frac{1}{x} \begin{pmatrix} 1/x & 0 \\ 0 & x \end{pmatrix},$$

which we can write as

$$\mathbf{A}^{-1} = \begin{pmatrix} 1/x & 0 \\ 0 & 1/(1/x) \end{pmatrix}.$$

This matrix is of the form

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

with $a = 1/x$. Also, $1/x \neq 0$. Hence $\mathbf{A}^{-1} \in P$.

Thus P contains the inverse of each of its elements.

Since the three subgroup properties hold, P is a subgroup of $\text{GL}(2)$. Hence it is a group under matrix multiplication.

(Another way to show that this set P is a subgroup of $\text{GL}(2)$ is to use Theorem B81 from Unit B4, which states that the intersection of two subgroups of a group is always a subgroup of the group.

The set P can be written as

$$P = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad = 1 \right\}.$$

So it is the set of all matrices in $\text{GL}(2)$ that are diagonal and have determinant 1. Hence it is the intersection of D , the set of diagonal matrices in $\text{GL}(2)$, and $\text{SL}(2)$, the set of matrices in $\text{GL}(2)$ with determinant 1. Each of these sets is a subgroup of $\text{GL}(2)$, by the results of Exercises E19 and E20 respectively, so it follows from Theorem B81 that P is also a subgroup of $\text{GL}(2)$.)

Solution to Exercise E22

Consider, for example, the matrix

$$\mathbf{A} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

This matrix is in X , because it is of the form

$$\begin{pmatrix} a & b \\ c & 1 \end{pmatrix}$$

with $a = 2$ and $b = c = 1$, and

$$a - bc = 2 - 1 \times 1 = 1 \neq 0.$$

However,

$$\mathbf{A}^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix},$$

and this matrix is not in X , because it is not of the form

$$\begin{pmatrix} a & b \\ c & 1 \end{pmatrix},$$

as its bottom right entry is not 1. Thus X is not closed under matrix multiplication.

Hence property SG1 fails, so X is not a subgroup of $\text{GL}(2)$.

Solution to Exercise E23

(a) $x^3 \circ x = x^4$ translates to

$$3x + x = 4x.$$

(b) $x^5 \circ x^{-5} = e$ translates to

$$5x + (-5)x = 0.$$

(c) $(x^4)^{-1} = (x^{-1})^4$ translates to

$$-(4x) = 4(-x).$$

Solution to Exercise E24

(a) (i) In $S(\square)$,

$$a^2 = a \circ a = b,$$

$$a^3 = a^2 \circ a = b \circ a = c,$$

$$a^4 = a^3 \circ a = c \circ a = e.$$

Thus a has order 4.

(ii) In $S(\square)$, $b^2 = e$, so b has order 2.

(iii) In $S(\square)$, $r^2 = e$, so r has order 2.

(b) The identity element of (U_9, \times_9) is 1.

(i) The consecutive powers of 5 in (U_9, \times_9) starting from 5^1 are

$$5^1, 5^2, 5^3, 5^4, 5^5, 5^6, \dots,$$

that is,

$$5, 7, 8, 4, 2, 1, \dots$$

So 5 has order 6 in (U_9, \times_9) .

(The first power in the list equal to 1 is the sixth power.)

(ii) The consecutive powers of 2 in (U_9, \times_9) starting from 2^1 are

$$2, 4, 8, 7, 5, 1, \dots$$

So 2 has order 6 in (U_9, \times_9) .

(Alternatively, the list of consecutive powers of 5 in part (b)(i) shows that $5^{-1} = 2$ in (U_9, \times_9) . Hence the order of 2 is the same as the order of 5, so the order of 2 is 6.)

To see why the list of consecutive powers of 5 shows that $5^{-1} = 2$ in (U_9, \times_9) , use the fact that each integer in the list is obtained by composing the previous integer with 5 in (U_9, \times_9) . The integer 1 appears immediately after the integer 2 in the list, so $2 \times_9 5 = 1$ and hence $5^{-1} = 2$.)

(iii) The consecutive powers of 7 in (U_9, \times_9) starting from 7^1 are

$$7, 4, 1, \dots$$

So 7 has order 3 in (U_9, \times_9) .

(The list of consecutive powers of 7 in (U_9, \times_9) can be obtained simply by working them out, or alternatively by using the list of powers of 5 in part (b)(i). If we start at $5^2 = 7$ in the list of powers of 5 and go forward two places at a time, then we obtain the powers

$$5^2, 5^4, 5^6, 5^8, \dots,$$

that is,

$$5^2, (5^2)^2, (5^2)^3, (5^2)^4, \dots$$

Hence we obtain the list of powers of $5^2 = 7$.)

(c) The group $(\mathbb{Z}_8, +_8)$ is additive, so the order of an element x in this group is the *smallest* positive integer n such that the *multiple* nx is equal to the identity element, 0.

(i) The consecutive multiples of 2 in $(\mathbb{Z}_8, +_8)$ starting from 1(2) are

$$1(2), 2(2), 3(2), 4(2), \dots,$$

that is,

$$2, 4, 6, 0, \dots$$

So 2 has order 4 in $(\mathbb{Z}_8, +_8)$.

(The first multiple in the list equal to 0 is the 4th multiple.)

(To calculate the consecutive multiples of 2 in $(\mathbb{Z}_8, +_8)$, we calculate

$$2(2) = 2 +_8 2 = 4,$$

$$3(2) = 2 +_8 2 +_8 2 = 6,$$

$$4(2) = 2 +_8 2 +_8 2 +_8 2 = 0,$$

and so on.

That is, we start with 2 and successively add 2 modulo 8 to each multiple to obtain the next multiple.)

(ii) The consecutive multiples of 3 in $(\mathbb{Z}_8, +_8)$ starting from 1(3) are

$$3, 6, 1, 4, 7, 2, 5, 0, \dots$$

So 3 has order 8 in $(\mathbb{Z}_8, +_8)$.

(iii) The consecutive multiples of 6 in $(\mathbb{Z}_8, +_8)$ starting from 1(6) are

$$6, 4, 2, 0, \dots$$

So 6 has order 4 in $(\mathbb{Z}_8, +_8)$.

(The fact that 6 has order 4 also follows from part (c)(i), since 6 is the inverse of 2 in $(\mathbb{Z}_8, +_8)$ and hence has the same order as 2.)

(An alternative way to find the orders of elements in a group $(\mathbb{Z}_n, +_n)$ is to use Theorem B38 from Unit B2, which you will revise in the next subsection.)

Solution to Exercise E25

The identity element of $GL(2)$ is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(a) In $GL(2)$,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4.

(b) The matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of $GL(2)$, so it has order 1.

(c) In $GL(2)$,

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ has order 2.

(d) In $GL(2)$,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^4 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}.$$

This pattern will continue because for any positive integer k we have

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}.$$

Hence in general for any positive integer n we have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

(This can be proved formally by using mathematical induction.)

Thus there is no positive integer n such that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order.

Solution to Exercise E26

(a) The permutation $(2\ 3)(6\ 9\ 8)$ has order 6.

(b) The permutation $(1\ 7\ 3\ 2\ 4)$ has order 5.

(c) The permutation $(1\ 7)(3\ 6\ 4\ 5)$ has order 4.

Solution to Exercise E27

In each case, the order of the cyclic subgroup is equal to the order of the group element that generates it. You found this order in Exercise E24, and in the same exercise you also worked out consecutive powers (or multiples) of this element, which give all the elements of the cyclic subgroup.

(a) The required cyclic subgroups of $S(\square)$ are as follows.

(i) $\langle a \rangle = \{e, a, b, c\}$

(ii) $\langle b \rangle = \{e, b\}$

(iii) $\langle r \rangle = \{e, r\}$

(The consecutive powers of a , b and r in $S(\square)$ are:

$$\dots, e, a, b, c, e, a, b, c, \dots,$$

$$\dots, e, b, e, b, e, b, \dots,$$

$$\dots, e, r, e, r, e, r, \dots)$$

(b) The required cyclic subgroups of (U_9, \times_9) are as follows.

(i) $\langle 5 \rangle = \{1, 5, 7, 8, 4, 2\}$

(ii) $\langle 2 \rangle = \{1, 2, 4, 8, 7, 5\}$ (Thus $\langle 2 \rangle = \langle 5 \rangle$.)

(iii) $\langle 7 \rangle = \{1, 7, 4\}$

(The consecutive powers of 5, 2 and 7 in (U_9, \times_9) are:

$$\dots, 1, 5, 7, 8, 4, 2, 1, 5, 7, 8, 4, 2, \dots,$$

$$\dots, 1, 2, 4, 8, 7, 5, 1, 2, 4, 8, 7, 5, \dots,$$

$$\dots, 1, 7, 4, 1, 7, 4, \dots)$$

(c) The required cyclic subgroups of $(\mathbb{Z}_8, +_8)$ are as follows.

(i) $\langle 2 \rangle = \{0, 2, 4, 6\}$

(ii) $\langle 3 \rangle = \{0, 3, 6, 1, 4, 7, 2, 5\}$ (Thus $\langle 3 \rangle = \mathbb{Z}_8$.)

(iii) $\langle 6 \rangle = \{0, 6, 4, 2\}$ (Thus $\langle 6 \rangle = \langle 2 \rangle$.)

(The consecutive multiples of 2, 3 and 6 in $(\mathbb{Z}_8, +_8)$ are:

$$\dots, 0, 2, 4, 6, 0, 2, 4, 6, \dots,$$

$$\dots, 0, 3, 6, 1, 4, 7, 2, 5, 0, 3, 6, 1, 4, 7, 2, 5, \dots,$$

$$\dots, 0, 6, 4, 2, 0, 6, 4, 2, \dots)$$

Solution to Exercise E28

(a) In $S(\square)$,

$$\langle e \rangle = \{e\},$$

$$\langle a \rangle = \{e, a, b, c\} = \langle c \rangle \quad (\text{since } c = a^{-1}),$$

$$\langle b \rangle = \{e, b\},$$

$$\langle r \rangle = \{e, r\},$$

$$\langle s \rangle = \{e, s\},$$

$$\langle t \rangle = \{e, t\},$$

$$\langle u \rangle = \{e, u\}.$$

Thus $S(\square)$ has seven distinct cyclic subgroups:

$$\{e\}, \quad \{e, a, b, c\},$$

$$\{e, b\}, \quad \{e, r\}, \quad \{e, s\}, \quad \{e, t\}, \quad \{e, u\}.$$

(As well as these seven cyclic subgroups, $S(\square)$ has three further subgroups, which are non-cyclic.

These are $S(\square)$ itself, and two subgroups of order 4, namely $\{e, b, r, t\}$ and $\{e, b, s, u\}$. The two non-cyclic subgroups of order 4 can be obtained by modifying the square, as given in the solution to Exercise E15(c).)

(b) In the additive group $(\mathbb{Z}_9, +_9)$,

$$\langle 0 \rangle = \{0\},$$

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \mathbb{Z}_9 = \langle 8 \rangle, \\ (\text{since } 8 \text{ is the inverse of } 1),$$

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 1, 3, 5, 7\} = \mathbb{Z}_9 = \langle 7 \rangle, \\ (\text{since } 7 \text{ is the inverse of } 2),$$

$$\langle 3 \rangle = \{0, 3, 6\} = \langle 6 \rangle, \\ (\text{since } 6 \text{ is the inverse of } 3),$$

$$\langle 4 \rangle = \{0, 4, 8, 3, 7, 2, 6, 1, 5\} = \mathbb{Z}_9 = \langle 5 \rangle, \\ (\text{since } 5 \text{ is the inverse of } 4).$$

Thus $(\mathbb{Z}_9, +_9)$ has three distinct cyclic subgroups:

$$\{0\}, \quad \{0, 3, 6\}, \quad \mathbb{Z}_9.$$

(c) In $(\mathbb{Z}_7^*, \times_7)$, we have $2 \times_7 4 = 1$, so 2 and 4 are inverses of each other, and $3 \times_7 5 = 1$, so 3 and 5 are inverses of each other.

In $(\mathbb{Z}_7^*, \times_7)$,

$$\langle 1 \rangle = \{1\},$$

$$\langle 2 \rangle = \{1, 2, 4\} = \langle 4 \rangle \quad (\text{since } 4 = 2^{-1}),$$

$$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^* = \langle 5 \rangle \quad (\text{since } 5 = 3^{-1}),$$

$$\langle 6 \rangle = \{1, 6\}.$$

Thus $(\mathbb{Z}_7^*, \times_7)$ has four distinct cyclic subgroups:

$$\{1\}, \quad \{1, 6\}, \quad \{1, 2, 4\}, \quad \mathbb{Z}_7^*.$$

(d) In S_3 ,

$$\langle e \rangle = \{e\},$$

$$\langle (1 \ 2) \rangle = \{e, (1 \ 2)\},$$

$$\langle (1 \ 3) \rangle = \{e, (1 \ 3)\},$$

$$\langle (2 \ 3) \rangle = \{e, (2 \ 3)\},$$

$$\langle (1 \ 2 \ 3) \rangle = \{e, (1 \ 2 \ 3), (1 \ 3 \ 2)\} = \langle (1 \ 3 \ 2) \rangle \\ (\text{since } (1 \ 2 \ 3)^{-1} = (1 \ 3 \ 2)).$$

Thus S_3 has five distinct cyclic subgroups:

$$\{e\}, \quad \{e, (1 \ 2)\}, \quad \{e, (1 \ 3)\}, \quad \{e, (2 \ 3)\}, \\ \{e, (1 \ 2 \ 3), (1 \ 3 \ 2)\}.$$

Solution to Exercise E29

(a) The group $S(\square)$ is non-cyclic because it has order 8 but contains no element of order 8:

the identity element has order 1,

the four reflections have order 2,

the rotation b has order 2,

the rotations a and c have order 4.

(b) The group $S^+(\square)$ is cyclic because it has order 4 and contains two elements (a and c) of order 4; each of these elements is a generator of the group.

(c) The group $(\mathbb{Z}_5, +_5)$ is cyclic because it has order 5 and contains four elements (1, 2, 3 and 4) of order 5; each of these elements is a generator of the group.

(d) We have

$$U_8 = \{1, 3, 5, 7\}.$$

We find the orders of the elements of (U_8, \times_8) .

The identity element 1 has order 1.

The consecutive powers of 3 are

$$\dots, 1, 3, 1, 3, \dots,$$

so 3 has order 2.

The consecutive powers of 5 are

$$\dots, 1, 5, 1, 5, \dots,$$

so 5 has order 2.

The consecutive powers of 7 are

$$\dots, 1, 7, 1, 7, \dots,$$

so 7 has order 2.

Thus (U_8, \times_8) has order 4 but contains no element of order 4, so it is non-cyclic.

Solution to Exercise E30

(a) By Theorem B38, the orders of the elements of $(\mathbb{Z}_{14}, +_{14})$ are as follows.

| Element | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---------|---|----|---|----|---|----|---|---|---|----|----|----|----|----|
| Order | 1 | 14 | 7 | 14 | 7 | 14 | 7 | 2 | 7 | 14 | 7 | 14 | 7 | 14 |

(b) By Corollary B40, or by the answers to part (a), the generators of $(\mathbb{Z}_{14}, +_{14})$ are 1, 3, 5, 9, 11 and 13.

Solution to Exercise E31

By Theorem B41, $(\mathbb{Z}_{16}, +_{16})$ has five subgroups, with orders 1, 2, 4, 8 and 16 (the factors of 16). They are:

$$\begin{aligned} \langle 0 \rangle &= \{0\}, \\ \langle 8 \rangle &= \{0, 8\}, \\ \langle 4 \rangle &= \{0, 4, 8, 12\}, \\ \langle 2 \rangle &= \{0, 2, 4, 6, 8, 10, 12, 14\}, \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \\ &\quad 11, 12, 13, 14, 15\} = \mathbb{Z}_{16}. \end{aligned}$$

Solution to Exercise E32

(a) $U_{10} = \{1, 3, 7, 9\}$.

| \times_{10} | 1 | 3 | 7 | 9 |
|---------------|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

(c) The group table found in part (b) can be rearranged as follows:

| \times_{10} | 1 | 3 | 9 | 7 |
|---------------|---|---|---|---|
| 1 | 1 | 3 | 9 | 7 |
| 3 | 3 | 9 | 7 | 1 |
| 9 | 9 | 7 | 1 | 3 |
| 7 | 7 | 1 | 3 | 9 |

This has the same pattern as the group table of $(\mathbb{Z}_4, +_4)$, which is

| $+_4$ | 0 | 1 | 2 | 3 |
|-------|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

An isomorphism from (U_{10}, \times_{10}) to $(\mathbb{Z}_4, +_4)$ is

$$\begin{aligned} \phi : U_{10} &\longrightarrow \mathbb{Z}_4 \\ 1 &\longmapsto 0 \\ 3 &\longmapsto 1 \\ 9 &\longmapsto 2 \\ 7 &\longmapsto 3. \end{aligned}$$

(The group table found in part (b) can also be rearranged as follows.

| \times_{10} | 1 | 7 | 9 | 3 |
|---------------|---|---|---|---|
| 1 | 1 | 7 | 9 | 3 |
| 7 | 7 | 9 | 3 | 1 |
| 9 | 9 | 3 | 1 | 7 |
| 3 | 3 | 1 | 7 | 9 |

This gives the following alternative isomorphism from (U_{10}, \times_{10}) to $(\mathbb{Z}_4, +_4)$:

$$\begin{aligned} \phi : U_{10} &\longrightarrow \mathbb{Z}_4 \\ 1 &\longmapsto 0 \\ 7 &\longmapsto 1 \\ 9 &\longmapsto 2 \\ 3 &\longmapsto 3. \end{aligned}$$

Solution to Exercise E33

Let ϕ be the mapping

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow 3\mathbb{Z} \\ n &\longmapsto 3n,\end{aligned}$$

as given in the question.

Then ϕ is one-to-one, because if m and n are elements of \mathbb{Z} such that $\phi(m) = \phi(n)$, then $3m = 3n$ and hence $m = n$.

Also, ϕ is onto, because any element of $3\mathbb{Z}$ is of the form $3n$ where $n \in \mathbb{Z}$, and this element is the image under ϕ of the element n of \mathbb{Z} .

Finally, if $m, n \in \mathbb{Z}$, then

$$\begin{aligned}\phi(m + n) &= 3(m + n) \\ &= 3m + 3n \\ &= \phi(m) + \phi(n).\end{aligned}$$

Thus ϕ is an isomorphism and hence $(\mathbb{Z}, +) \cong (3\mathbb{Z}, +)$.

Solution to Exercise E34

The group (G, \times) from Exercise E3 is a group of order 4 all of whose elements are self-inverse.

Therefore it is isomorphic to the Klein four-group V (and $S(\square)$).

Solution to Exercise E35

We have

$$U_{18} = \{1, 5, 7, 11, 13, 17\}.$$

Thus U_{18} is a group of order 6. It is abelian, since \times_{18} is a commutative binary operation. Therefore it is isomorphic to \mathbb{Z}_6 (and C_6).

Solution to Exercise E36

(a) The left cosets of $\{e, s\}$ in $S(\triangle)$ are

$$\begin{aligned}eH &= \{e \circ e, e \circ s\} = \{e, s\} = H, \\ aH &= \{a \circ e, a \circ s\} = \{a, r\}, \\ bH &= \{b \circ e, b \circ s\} = \{b, t\}, \\ rH &= \{r \circ e, r \circ s\} = \{r, a\}, \\ sH &= \{s \circ e, s \circ s\} = \{s, e\} = H, \\ tH &= \{t \circ e, t \circ s\} = \{t, b\}.\end{aligned}$$

(b) The distinct left cosets of $H = \{e, s\}$ in $S(\triangle)$ are

$$\{e, s\}, \quad \{a, r\}, \quad \{b, t\}.$$

Solution to Exercise E37

(a) The consecutive powers of 2 in \mathbb{Z}_7^* starting from 2^1 are

$$2, 4, 1, \dots$$

Thus $\langle 2 \rangle = \{1, 2, 4\}$. That is, $H = \{1, 2, 4\}$ is the cyclic subgroup of \mathbb{Z}_7^* generated by 2.

(b) The left cosets of $H = \{1, 2, 4\}$ in \mathbb{Z}_7^* are

$$\begin{aligned}1H &= \{1 \times_7 1, 1 \times_7 2, 1 \times_7 4\} = \{1, 2, 4\} = H, \\ 2H &= \{2 \times_7 1, 2 \times_7 2, 2 \times_7 4\} = \{2, 4, 1\} = H, \\ 3H &= \{3 \times_7 1, 3 \times_7 2, 3 \times_7 4\} = \{3, 6, 5\}, \\ 4H &= \{4 \times_7 1, 4 \times_7 2, 4 \times_7 4\} = \{4, 1, 2\} = H, \\ 5H &= \{5 \times_7 1, 5 \times_7 2, 5 \times_7 4\} = \{5, 3, 6\}, \\ 6H &= \{6 \times_7 1, 6 \times_7 2, 6 \times_7 4\} = \{6, 5, 3\}.\end{aligned}$$

(c) The distinct left cosets of $H = \{1, 2, 4\}$ in \mathbb{Z}_7^* are

$$\{1, 2, 4\}, \quad \{3, 5, 6\}.$$

Solution to Exercise E38

(a) The subgroup $H = \{e, a, b, c\}$ is one left coset, by Proposition E3(b).

All the left cosets of H contain the same number of elements as H by Proposition E3(d), and distinct left cosets are disjoint from each other by Proposition E3(c).

It follows that there is just one other left coset, namely $\{r, s, t, u\}$.

So the distinct left cosets of H in $S(\square)$ are

$$\{e, a, b, c\}, \quad \{r, s, t, u\}.$$

(b) All the left cosets of H contain the same number of elements by Proposition E3(d).

Thus each left coset of the subgroup $H = \{e\}$ has just one element.

Hence there are eight distinct left cosets of H in $S(\square)$, each with one element:

$$\{e\}, \{a\}, \{b\}, \{c\}, \{r\}, \{s\}, \{t\}, \{u\}.$$

(c) The subgroup $S(\square)$ is the whole group, and so is the only left coset by Proposition E3(b) and (c).

Solution to Exercise E39

We have

$$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}.$$

Also,

$$19 \times 19 \equiv (-1) \times (-1) \equiv 1 \pmod{20},$$

so

$$19 \times_{20} 19 = 1.$$

Hence $\langle 19 \rangle = \{1, 19\}$, so $H = \{1, 19\}$ is the cyclic subgroup of U_{20} generated by 19.

By Strategy E1, the left cosets of $H = \{1, 19\}$ in U_{20} are

$$\begin{aligned} H &= \{1, 19\}, \\ 3H &= \{3 \times_{20} 1, 3 \times_{20} 19\} = \{3, 17\}, \\ 7H &= \{7 \times_{20} 1, 7 \times_{20} 19\} = \{7, 13\}, \\ 9H &= \{9 \times_{20} 1, 9 \times_{20} 19\} = \{9, 11\}. \end{aligned}$$

The partition of U_{20} into left cosets of H is therefore

$$\{1, 19\}, \quad \{3, 17\}, \quad \{7, 13\}, \quad \{9, 11\}.$$

(A quick way of obtaining the second element in each of the left cosets above is as follows:

$$\begin{aligned} 3 \times 19 &\equiv 3 \times (-1) \equiv -3 \equiv 17 \pmod{20}, \\ 7 \times 19 &\equiv 7 \times (-1) \equiv -7 \equiv 13 \pmod{20}, \\ 9 \times 19 &\equiv 9 \times (-1) \equiv -9 \equiv 11 \pmod{20}. \end{aligned}$$

Solution to Exercise E40

By Strategy E1, the left cosets of $H = \{e, t\}$ in $S(\triangle)$ are

$$\begin{aligned} H &= \{e, t\}, \\ aH &= \{a \circ e, a \circ t\} = \{a, s\}, \\ bH &= \{b \circ e, b \circ t\} = \{b, r\}. \end{aligned}$$

The partition of $S(\triangle)$ into left cosets of H is therefore

$$\{e, t\}, \quad \{a, s\}, \quad \{b, r\}.$$

Solution to Exercise E41

Using Strategy E1, we find that the left cosets of H in A_4 are

$$\begin{aligned} H &= \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \\ (1\ 2\ 3)H &= \{(1\ 2\ 3) \circ e, (1\ 2\ 3) \circ (1\ 2)(3\ 4), \\ &\quad (1\ 2\ 3) \circ (1\ 3)(2\ 4), (1\ 2\ 3) \circ (1\ 4)(2\ 3)\} \\ &= \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}, \\ (1\ 3\ 2)H &= \{(1\ 3\ 2) \circ e, (1\ 3\ 2) \circ (1\ 2)(3\ 4), \\ &\quad (1\ 3\ 2) \circ (1\ 3)(2\ 4), (1\ 3\ 2) \circ (1\ 4)(2\ 3)\} \\ &= \{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\}. \end{aligned}$$

In summary, the partition into left cosets is

$$\begin{aligned} &\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \\ &\{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}, \\ &\{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\}. \end{aligned}$$

Solution to Exercise E42

The right cosets of $H = \{e, s\}$ in $S(\triangle)$ are

$$\begin{aligned} H &= \{e, s\}, \\ Ha &= \{e \circ a, s \circ a\} = \{a, t\}, \\ Hb &= \{e \circ b, s \circ b\} = \{b, r\}. \end{aligned}$$

The partition of $S(\triangle)$ into right cosets of H is therefore

$$\{e, s\}, \quad \{a, t\}, \quad \{b, r\}.$$

Solution to Exercise E43

\Rightarrow part

Suppose that

$$x \in yH.$$

Then

$$x = yh$$

for some $h \in H$. Composing each side of this equation with x^{-1} on the right gives

$$xx^{-1} = yhx^{-1},$$

that is,

$$e = yhx^{-1}.$$

Now composing each side of this equation with y^{-1} on the left gives

$$y^{-1}e = y^{-1}yhx^{-1},$$

that is,

$$y^{-1} = hx^{-1}.$$

Hence $y^{-1} \in Hx^{-1}$, as required.

⇐ **part**

Now suppose that

$$y^{-1} \in Hx^{-1}.$$

Then

$$y^{-1} = hx^{-1}$$

for some $h \in H$. Composing each side of this equation with x on the right gives

$$y^{-1}x = hx^{-1}x,$$

that is,

$$y^{-1}x = h.$$

Now composing each side of this equation with y on the left gives

$$yy^{-1}x = yh,$$

that is,

$$x = yh.$$

Hence $x \in yH$, as required.

This completes the proof.

Solution to Exercise E44

(a) Using Strategy E1, we find that the cosets are

$$H = \{0, 2, 4, 6, 8\},$$

$$1 + H$$

$$= 1 + \{0, 2, 4, 6, 8\}$$

$$= \{1 +_{10} 0, 1 +_{10} 2, 1 +_{10} 4, 1 +_{10} 6, 1 +_{10} 8\}$$

$$= \{1, 3, 5, 7, 9\}.$$

In summary, the partition is

$$\{0, 2, 4, 6, 8\}, \quad \{1, 3, 5, 7, 9\}.$$

(In fact, there is no need to work out the second coset in the way above, because the group \mathbb{Z}_{10} and the subgroup H have orders 10 and 5, respectively, so there are two cosets each containing 5 elements, and hence the second coset contains all the elements of \mathbb{Z}_{10} that are not in the first coset H .)

(b) Using Strategy E1, we find that the cosets are

$$H = \{0, 5\},$$

$$1 + H = 1 + \{0, 5\}$$

$$= \{1 +_{10} 0, 1 +_{10} 5\}$$

$$= \{1, 6\},$$

$$2 + H = 2 + \{0, 5\}$$

$$= \{2 +_{10} 0, 2 +_{10} 5\}$$

$$= \{2, 7\},$$

$$3 + H = 3 + \{0, 5\}$$

$$= \{3 +_{10} 0, 3 +_{10} 5\}$$

$$= \{3, 8\},$$

$$4 + H = 4 + \{0, 5\}$$

$$= \{4 +_{10} 0, 4 +_{10} 5\}$$

$$= \{4, 9\}.$$

In summary, the partition is

$$\{0, 5\}, \quad \{1, 6\}, \quad \{2, 7\}, \quad \{3, 8\}, \quad \{4, 9\}.$$

(Similarly to part (a), there is no need to work out the final coset in the way above, as it must contain the two elements of \mathbb{Z}_{10} not yet assigned to a coset. However, working out the final coset is a useful check.)

Solution to Exercise E45

(a) The cosets of $4\mathbb{Z}$ in \mathbb{Z} are

$$4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\},$$

$$1 + 4\mathbb{Z} = \{\dots, -7, -3, 1, 5, 9, \dots\},$$

$$2 + 4\mathbb{Z} = \{\dots, -6, -2, 2, 6, 10, \dots\},$$

$$3 + 4\mathbb{Z} = \{\dots, -5, -1, 3, 7, 11, \dots\}.$$

(b) The cosets of $6\mathbb{Z}$ in $2\mathbb{Z}$ are

$$6\mathbb{Z} = \{\dots, -12, -6, 0, 6, 12, \dots\},$$

$$2 + 6\mathbb{Z} = \{\dots, -10, -4, 2, 8, 14, \dots\},$$

$$4 + 6\mathbb{Z} = \{\dots, -8, -2, 4, 10, 16, \dots\}.$$

(Here the whole group $2\mathbb{Z}$ consists of only the *even* integers, so there are no cosets such as $1 + 6\mathbb{Z}$.)

Solution to Exercise E46

(a) By Exercise E40, the partition of $S(\triangle)$ into left cosets of the subgroup $\{e, t\}$ is

$$\{e, t\}, \quad \{a, s\}, \quad \{b, r\}.$$

In $S(\triangle)$ the elements a and b are inverses of each other and all the other elements are self-inverse. So the partition of $S(\triangle)$ into right cosets of the subgroup $\{e, t\}$ is

$$\{e, t\}, \quad \{b, s\}, \quad \{a, r\},$$

that is,

$$\{e, t\}, \quad \{a, r\}, \quad \{b, s\}.$$

Since the two partitions are different, $\{e, t\}$ is not a normal subgroup of $S(\triangle)$.

(b) All the left cosets of the subgroup $S^+(\triangle) = \{e, a, b\}$ in $S(\triangle)$ contain three elements and one of the left cosets is the subgroup itself, and the same is true for the right cosets. So the partition of $S(\triangle)$ into left cosets of $\{e, a, b\}$ and the partition of $S(\triangle)$ into right cosets of $\{e, a, b\}$ are both

$$\{e, a, b\}, \quad \{r, s, t\}.$$

Since the two partitions are the same, $S^+(\triangle) = \{e, a, b\}$ is a normal subgroup of $S(\triangle)$.

(c) Every left coset and every right coset of the subgroup $\{e\}$ in $S(\triangle)$ contains just one element, so the partition of $S(\triangle)$ into left cosets of $\{e\}$ and the partition of $S(\triangle)$ into right cosets of $\{e\}$ are both

$$\{e\}, \{a\}, \{b\}, \{r\}, \{s\}, \{t\}.$$

Since the two partitions are the same, $\{e\}$ is a normal subgroup of $S(\triangle)$.

(d) The only left coset and the only right coset of $S(\triangle)$ in $S(\triangle)$ is $S(\triangle)$.

So the partition into left cosets and the partition into right cosets are both simply $S(\triangle)$.

Since the two partitions are the same, $S(\triangle)$ is a normal subgroup of $S(\triangle)$.

Solution to Exercise E47

(a) The left coset $(1\ 2)(3\ 4)H$ is

$$\begin{aligned} & (1\ 2)(3\ 4)H \\ &= \{(1\ 2)(3\ 4) \circ e, (1\ 2)(3\ 4) \circ (1\ 2\ 3), \\ & \quad (1\ 2)(3\ 4) \circ (1\ 3\ 2)\} \\ &= \{(1\ 2)(3\ 4), (2\ 4\ 3), (1\ 4\ 3)\}. \end{aligned}$$

The right coset $H(1\ 2)(3\ 4)$ is

$$\begin{aligned} & H(1\ 2)(3\ 4) \\ &= \{e \circ (1\ 2)(3\ 4), (1\ 2\ 3) \circ (1\ 2)(3\ 4), \\ & \quad (1\ 3\ 2) \circ (1\ 2)(3\ 4)\} \\ &= \{(1\ 2)(3\ 4), (1\ 3\ 4), (2\ 3\ 4)\}. \end{aligned}$$

So the left coset $(1\ 2)(3\ 4)H$ and the right coset $H(1\ 2)(3\ 4)$ are not the same. Since the permutation $(1\ 2)(3\ 4)$ lies in both these cosets, the partition of A_4 into left cosets of H is not the same as its partition into right cosets of H . Hence H is not a normal subgroup of A_4 .

(b) By the solution to Exercise E41, the left cosets of K in A_4 are

$$\begin{aligned} & \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \\ & \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}, \\ & \{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\}. \end{aligned}$$

By replacing each permutation by its inverse, we find that the right cosets of K in A_4 are

$$\begin{aligned} & \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \\ & \{(1\ 3\ 2), (1\ 4\ 3), (2\ 3\ 4), (1\ 2\ 4)\}, \\ & \{(1\ 2\ 3), (2\ 4\ 3), (1\ 4\ 2), (1\ 3\ 4)\}. \end{aligned}$$

These are the same sets as in the partition into left cosets (just in a different order and with their elements listed in a different order). So the partition of A_4 into left cosets of K and the partition of A_4 into right cosets of K are the same. Hence K is a normal subgroup of A_4 .

Solution to Exercise E48

(a) The group $(\mathbb{Z}, +)$ is abelian, so all of its subgroups are normal, and hence in particular its subgroup $4\mathbb{Z}$ is normal.

(b) In any symmetry group, either all the symmetries are direct or half are direct and half are indirect, by Theorem B22. The regular tetrahedron has some indirect symmetries, such as the reflection in the plane that passes through two vertices and the midpoint of the edge joining the other two vertices, so half of its symmetries are direct and half are indirect. Hence the subgroup of direct symmetries of $S(\text{tet})$ is a subgroup of index 2, and therefore it is a normal subgroup.

(c) The 4-windmill has no indirect symmetries, so its subgroup of direct symmetries is equal to the whole group $S(\text{4w})$ and hence is a normal subgroup.

Unit E2

Quotient groups and conjugacy

Introduction

In the final section of the previous unit you met the idea of a *normal subgroup*. This next unit covers two topics that are both related to normal subgroups.

In the first section you will study *quotient groups*. You will see that if G is a group with a normal subgroup N then, in a sense that you will learn about, we can ‘divide’ G by N to obtain a *quotient group* G/N .

Essentially, the group G can be ‘broken down’ into two groups N and G/N . You can think of the process as being similar to the way that if g is a natural number with a positive divisor n , then g can be broken down into the two numbers n and g/n : for example, the number 12 can be broken down into the numbers 4 and $12/4 = 3$.

In the other four sections you will learn how the idea of *conjugacy*, which you met in the context of symmetric groups in Unit B3 *Permutations*, can be generalised to all groups. As you will see, conjugacy can help us to understand the relationships between different elements of the same group. It also gives us useful methods for determining whether or not a subgroup of a group is a normal subgroup, and it can help us find more subgroups of a group once we know some subgroups.

This is a substantial unit, so you should expect to spend longer studying it than you would for a typical group theory unit. The next unit, Unit E3, is much shorter.

1 Quotient groups

In this section you will see that if G is a group with a normal subgroup N then we can form a new group whose elements are the cosets of N in G . We denote this group by G/N and call it a *quotient group* of G .

1.1 What is a quotient group?

Before you can learn more about quotient groups, you need to learn about the idea of *set composition* in a group. This is the binary operation of any quotient group of the group.

Given any group G , we can use its binary operation to obtain a related binary operation, known as set composition, that is defined on the set of *subsets* of G . That is, this new binary operation is a way of combining any two subsets of G to give another subset of G . It is defined below.

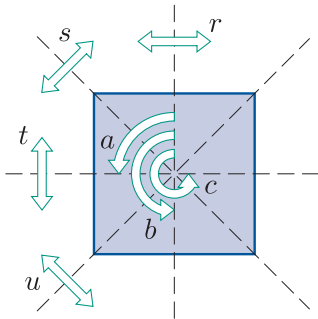


Figure 1 The symmetries of the square

Table 1 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

Definition

Let G be a group. Then the binary operation \cdot , called **set composition** in G , is defined on the set of subsets of G by

$$X \cdot Y = \{xy : x \in X, y \in Y\}$$

for all subsets X and Y of G .

That is, if X and Y are subsets of G then $X \cdot Y$ is the subset of G obtained by composing each element of X with each element of Y , in that order.

Worked Exercise E19

Determine the following composites of subsets in the group $S(\square)$.

(The non-identity symmetries of the square are shown in Figure 1 and the group table of $S(\square)$ is given as Table 1.)

- (a) $\{s, u\} \cdot \{r, t\}$ (b) $\{b, t\} \cdot \{c, u\}$

Solution

$$\begin{aligned} \text{(a) } \{s, u\} \cdot \{r, t\} &= \{s \circ r, s \circ t, u \circ r, u \circ t\} \\ &= \{a, c, c, a\} \\ &= \{a, c\} \end{aligned}$$

$$\begin{aligned} \text{(b) } \{b, t\} \cdot \{c, u\} &= \{b \circ c, b \circ u, t \circ c, t \circ u\} \\ &= \{a, s, u, c\} \end{aligned}$$

Notice from Worked Exercise E19 that when we use set composition to combine two subsets of a group G we may obtain repeated elements. However, we write the resulting set with each element appearing just once, since a set does not contain repeated elements. The order in which we write the elements does not matter, since the elements of a set can be written in any order.

Exercise E49

Determine the following composites of subsets in $S(\square)$.

- (a) $\{e, b\} \cdot \{r, t\}$ (b) $\{a, c\} \cdot \{a, c\}$ (c) $\{a, s\} \cdot \{a, s\}$
(d) $\{a, s\} \cdot \{a, s, e\}$

For an *additive* group G , we denote set composition by $+$ rather than \cdot , as illustrated in the next worked exercise.

Worked Exercise E20

Determine the composite of subsets $\{1, 4, 7\} + \{2, 5, 8\}$ in the group \mathbb{Z}_9 .

Solution

$$\begin{aligned}\{1, 4, 7\} + \{2, 5, 8\} &= \{1 +_9 2, 1 +_9 5, 1 +_9 8, \\ &\quad 4 +_9 2, 4 +_9 5, 4 +_9 8, \\ &\quad 7 +_9 2, 7 +_9 5, 7 +_9 8\} \\ &= \{3, 6, 0, 6, 0, 3, 0, 3, 6\} \\ &= \{0, 3, 6\}\end{aligned}$$

Exercise E50

Determine the following composites of subsets in the group \mathbb{Z}_9 .

- (a) $\{1, 4, 7\} + \{1, 4, 7\}$ (b) $\{0, 3, 6\} + \{1, 4, 7\}$

Set composition in an abelian group is a commutative binary operation, since for any two subsets X and Y of an abelian group we have

$$\begin{aligned}X \cdot Y &= \{xy : x \in X, y \in Y\} \\ &= \{yx : y \in Y, x \in X\} \\ &= Y \cdot X.\end{aligned}$$

On the other hand, set composition in a non-abelian group is a non-commutative binary operation, since a non-abelian group contains elements x and y such that $xy \neq yx$, and

$$\{x\} \cdot \{y\} = \{xy\}$$

whereas

$$\{y\} \cdot \{x\} = \{yx\}.$$

Exercise E51

Show that, in $S(\square)$,

$$\{b, t\} \cdot \{c, u\} \neq \{c, u\} \cdot \{b, t\}.$$

(The composite on the left here was found in Worked Exercise E19(b). The group table of $S(\square)$ is given as Table 2.)

Table 2 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

Although set composition is defined for any two subsets of a group, we will mainly be interested in applying it to *cosets of normal subgroups*. (You met the ideas of cosets and normal subgroups in Sections 4 and 5 of Unit E1 *Cosets and normal subgroups*.) Remember that for normal subgroups we refer simply to *cosets* rather than *left cosets* or *right cosets*, because for normal subgroups left cosets and right cosets are the same.

Let us look at what happens when we use set composition to compose two cosets of the same normal subgroup of a group.

Consider the example of the group $S(\square)$ and its normal subgroup $\{e, b\}$. You saw that this subgroup is normal in Worked Exercise E18 in Section 5 of Unit E1. We found there that its cosets are

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

Let us look at what happens when we use set composition to compose two of these four cosets.

For example, we have

$$\begin{aligned} \{a, c\} \cdot \{r, t\} &= \{a \circ r, a \circ t, c \circ r, c \circ t\} \\ &= \{s, u, u, s\} \\ &= \{s, u\}. \end{aligned}$$

This composite has turned out to be equal to one of the four cosets.

In fact we have already composed some other pairs of these four cosets. In Worked Exercise E19 and Exercise E49 we found that

$$\begin{aligned} \{s, u\} \cdot \{r, t\} &= \{a, c\}, \\ \{e, b\} \cdot \{r, t\} &= \{r, t\}, \\ \{a, c\} \cdot \{a, c\} &= \{e, b\}. \end{aligned}$$

Again, each of these composites is equal to one of the four cosets. In the next exercise you are asked to investigate whether composing a pair of the four cosets always gives one of the four cosets.

Exercise E52

Table 3 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

- (a) Complete the Cayley table below for the cosets of the normal subgroup $\{e, b\}$ of $S(\square)$ under set composition. The composites already entered are those given above and some others that have been worked out for you to save you time.

(The group table of $S(\square)$ is given as Table 3.)

| \cdot | $\{e, b\}$ | $\{a, c\}$ | $\{r, t\}$ | $\{s, u\}$ |
|------------|------------|------------|------------|------------|
| $\{e, b\}$ | | $\{a, c\}$ | $\{r, t\}$ | $\{s, u\}$ |
| $\{a, c\}$ | $\{a, c\}$ | $\{e, b\}$ | $\{s, u\}$ | |
| $\{r, t\}$ | $\{r, t\}$ | | $\{e, b\}$ | $\{a, c\}$ |
| $\{s, u\}$ | $\{s, u\}$ | $\{r, t\}$ | $\{a, c\}$ | |

- (b) Check whether all the sets in the body of the table are cosets of $\{e, b\}$ in $S(\square)$.

Exercise E52 shows that composing a pair of cosets of $\{e, b\}$ in $S(\square)$ always gives a coset of $\{e, b\}$ in $S(\square)$: in other words, the set of cosets of $\{e, b\}$ in $S(\square)$ is closed under set composition.

In the next exercise you are asked to determine whether the set of cosets of the normal subgroup $\{0, 3, 6\}$ of the additive group \mathbb{Z}_9 is also closed under set composition. This set is a subgroup of \mathbb{Z}_9 because it is the cyclic subgroup generated by 3, and it is normal in \mathbb{Z}_9 because \mathbb{Z}_9 is abelian. (By Theorem E10 in Unit E1, every subgroup of an abelian group is normal.)

Exercise E53

- (a) Complete the Cayley table below for the cosets of the normal subgroup $\{0, 3, 6\}$ of the group \mathbb{Z}_9 under set composition.

(The composites already entered were obtained in Worked Exercise E20 and Exercise E50. Remember that set composition in \mathbb{Z}_9 is commutative, because \mathbb{Z}_9 is abelian, so to complete the table you have to work out only three composites, not four.)

| + | $\{0, 3, 6\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ |
|---------------|---------------|---------------|---------------|
| $\{0, 3, 6\}$ | | $\{1, 4, 7\}$ | |
| $\{1, 4, 7\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ | $\{0, 3, 6\}$ |
| $\{2, 5, 8\}$ | | $\{0, 3, 6\}$ | |

- (b) Check whether all the sets in the body of the table are cosets of $\{0, 3, 6\}$ in \mathbb{Z}_9 .

Exercises E52 and E53 seem to suggest that if N is a normal subgroup of a group G , then the set of cosets of N in G is always closed under set composition. This is indeed the case, as is confirmed by the theorem below. This theorem says that if we compose the coset of N that contains the element x with the coset of N that contains the element y , in that order, then we obtain the coset of N that contains the element xy .

Of course, if we compose the coset of N that contains the element x with the coset of N that contains the element y , in that order, then we will obtain a *set* that contains the element xy : this follows immediately from the definition of set composition. The significance of the theorem is that the set that we obtain is always a *coset* of N .

Theorem E14

Let N be a normal subgroup of a group G . Then, for all $x, y \in G$,

$$xN \cdot yN = (xy)N.$$

Proof Let $x, y \in G$. To show that the two sets $xN \cdot yN$ and $(xy)N$ are equal, we show that $xN \cdot yN \subseteq (xy)N$ and $(xy)N \subseteq xN \cdot yN$.

Proof that $xN \cdot yN \subseteq (xy)N$

Let $z \in xN \cdot yN$. Then

$$z = xn_1yn_2$$

for some $n_1, n_2 \in N$. We have to show that $z \in (xy)N$.

Consider the expression n_1y that occurs in the middle of the expression for z above. We know that $n_1y \in Ny$, and we know that $Ny = yN$, since N is a normal subgroup. Therefore $n_1y \in yN$. It follows that there is some element n_3 , say, of N such that

$$n_1y = yn_3.$$

Using this equation to replace the expression n_1y in the expression for z above gives

$$z = xyn_3n_2.$$

Now $n_3n_2 \in N$, since N is a subgroup, so we can conclude that $z \in (xy)N$.

Hence $xN \cdot yN \subseteq (xy)N$.

Proof that $(xy)N \subseteq xN \cdot yN$

Let $z \in (xy)N$. Then

$$z = xyn$$

for some $n \in N$. Since $x \in xN$ and $yn \in yN$, it follows that

$$z \in xN \cdot yN.$$

Hence $(xy)N \subseteq xN \cdot yN$.

This completes the proof that $xN \cdot yN = (xy)N$. ■

So we now know the following fact:

If N is a normal subgroup of a group G , then the set of cosets of N in G is closed under set composition.

Before we consider cosets of normal subgroups further, let us consider whether a similar fact might hold for subgroups that are *not normal*. Might it be true that if H is *any* subgroup of a group G , then the set of left cosets of H in G is always closed under set composition, and the set of right cosets of H in G is always closed under set composition? In fact this is not true, as you are asked to show in the next exercise. So Theorem E14 cannot be generalised to include subgroups that are not normal.

Exercise E54

The left cosets of the subgroup $\{e, r\}$ in the group $S(\square)$ are

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\},$$

and the right cosets are

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

Find counterexamples to show that the set of left cosets of $\{e, r\}$ is not closed under set composition in $S(\square)$, and neither is the set of right cosets.

(The cosets of the subgroup $\{e, r\}$ in $S(\square)$ were found in Worked Exercises E12 and E15 in Subsections 4.1 and 4.2 of Unit E1. The group table of $S(\square)$ is given as Table 4.)

Table 4 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

So far in this subsection we have found that if N is a normal subgroup of a group G , then the set of cosets of N in G is closed under set composition. In other words, it satisfies group axiom G1. In fact even more is true: the set of cosets with set composition also satisfies the other three group axioms and hence *is a group*. You will see a proof of this fact shortly, but first, to illustrate it, let us look again at the Cayley tables that you should have found in Exercises E52 and E53.

The Cayley table for the cosets of the normal subgroup $\{e, b\}$ in $S(\square)$ is as follows.

| \cdot | $\{e, b\}$ | $\{a, c\}$ | $\{r, t\}$ | $\{s, u\}$ |
|------------|------------|------------|------------|------------|
| $\{e, b\}$ | $\{e, b\}$ | $\{a, c\}$ | $\{r, t\}$ | $\{s, u\}$ |
| $\{a, c\}$ | $\{a, c\}$ | $\{e, b\}$ | $\{s, u\}$ | $\{r, t\}$ |
| $\{r, t\}$ | $\{r, t\}$ | $\{s, u\}$ | $\{e, b\}$ | $\{a, c\}$ |
| $\{s, u\}$ | $\{s, u\}$ | $\{r, t\}$ | $\{a, c\}$ | $\{e, b\}$ |

In this table the row and column labelled by the coset $\{e, b\}$ both repeat the table borders. So the coset $\{e, b\}$ (this coset is the normal subgroup itself) is an identity element for set composition on the set of cosets. The table also shows that each coset has an inverse under set composition: in fact each coset is self-inverse, since the identity element $\{e, b\}$ appears in each position on the main diagonal. It is also true that set composition is associative; this follows from the fact that the original group operation is associative, as you will see proved formally shortly. So the Cayley table is a group table. The group in the Cayley table is isomorphic to the Klein four-group V , since it has order 4 and all its elements are self-inverse. (Distinguishing features for isomorphism classes of groups of orders 1 to 8 are given in Subsection 3.4 of Unit E1.)

Now let us look at the Cayley table for the cosets of the normal subgroup $\{0, 3, 6\}$ in the additive group \mathbb{Z}_9 , which is as follows.

| + | $\{0, 3, 6\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ |
|---------------|---------------|---------------|---------------|
| $\{0, 3, 6\}$ | $\{0, 3, 6\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ |
| $\{1, 4, 7\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ | $\{0, 3, 6\}$ |
| $\{2, 5, 8\}$ | $\{2, 5, 8\}$ | $\{0, 3, 6\}$ | $\{1, 4, 7\}$ |

You can check in a similar way to the argument above that this Cayley table is a group table. Again the identity element is the normal subgroup itself, namely $\{0, 3, 6\}$ here. This time, however, the other elements are not self-inverse. The group in the table is isomorphic to the cyclic group C_3 .

When we construct a Cayley table for a set of cosets, like those above, it is usually more convenient to denote the cosets by using notation of the form xN , rather than by listing the elements of each coset. If we do this for the two Cayley tables above, then we obtain the following tables.

The Cayley table for the cosets of $N = \{e, b\}$ in $S(\square)$ is as follows.

| \cdot | N | aN | rN | sN |
|---------|------|------|------|------|
| N | N | aN | rN | sN |
| aN | aN | N | sN | rN |
| rN | rN | sN | N | aN |
| sN | sN | rN | aN | N |

The Cayley table for the cosets of $N = \{0, 3, 6\}$ in \mathbb{Z}_9 is as follows.

| + | N | $1 + N$ | $2 + N$ |
|---------|---------|---------|---------|
| N | N | $1 + N$ | $2 + N$ |
| $1 + N$ | $1 + N$ | $2 + N$ | N |
| $2 + N$ | $2 + N$ | N | $1 + N$ |

In Cayley tables like these, it is important to denote each coset in a consistent way throughout the table. For example, in the Cayley table for the cosets of $N = \{e, b\}$ in $S(\square)$, the coset $\{a, c\}$ could be written either as aN or cN , but it is important to choose one of these two possibilities and use it for every occurrence of the coset $\{a, c\}$ in the table. This makes the structure of the group clearer.

Now here is the proof that the cosets of a normal subgroup always form a group under set composition.

Theorem E15

Let N be a normal subgroup of a group G . Then the set of cosets of N in G , with the binary operation of set composition, is a group.

Proof We show that the set of cosets of N in G , with the binary operation of set composition, satisfies the four group axioms.

G1 Closure

By Theorem E14, the set of cosets of N in G is closed under set composition.

G2 Associativity

Let xN , yN and zN be any cosets of N in G . Then, by Theorem E14, and since the binary operation of G is associative,

$$xN \cdot (yN \cdot zN) = xN \cdot (yz)N = (x(yz))N = (xyz)N,$$

and

$$(xN \cdot yN) \cdot zN = (xy)N \cdot zN = ((xy)z)N = (xyz)N.$$

Since the two expressions obtained are the same, set composition is associative on the set of cosets of N in G .

G3 Identity

Let e be the identity element in G . Then, by Theorem E14, for each coset xN of N in G ,

$$xN \cdot eN = (xe)N = xN,$$

and

$$eN \cdot xN = (ex)N = xN.$$

This shows that the coset eN , which is equal to N , is an identity element for set composition on the set of cosets of N in G .

G4 Inverses

Let xN be any coset of N in G . Since x is an element of the group G , it has an inverse element x^{-1} in G . Now, by Theorem E14,

$$xN \cdot x^{-1}N = (xx^{-1})N = eN = N,$$

and

$$x^{-1}N \cdot xN = (x^{-1}x)N = eN = N.$$

Since N is an identity element, this shows that $x^{-1}N$ is an inverse of xN with respect to set composition. Thus each coset of N has an inverse element in the set of cosets of N in G with respect to set composition.

Hence the set of cosets of N in G , with the binary operation of set composition, satisfies the four group axioms and so is a group. ■

The group formed by the cosets of a normal subgroup N of a group G is called the **quotient group** (or **factor group**) of G by N , and is denoted by G/N . In this context the notation G/N is pronounced as ‘ G modulo N ’ or ‘ $G \bmod N$ ’ for short, or simply as ‘ G over N ’.

If G is a *finite* group, then the number of cosets of N in G is $|G|/|N|$, since each coset of N contains the same number of elements as N , and hence the quotient group of G by N has order $|G|/|N|$. For example, as you have seen, the group formed by the cosets of $\{e, b\}$ in $S(\square)$ has order $8/2 = 4$, and the group formed by the cosets of $\{0, 3, 6\}$ in \mathbb{Z}_9 has order $9/3 = 3$.

More generally, for any group G , finite or infinite, and any normal subgroup N of G :

- if N has r cosets in G , then G/N has order r
- if N has infinitely many cosets in G , then G/N has infinite order.

In other words, the order of G/N is equal to the *index* of N in G .

Here is a summary of the important facts that we have established in this subsection.

Quotient groups

Let N be a normal subgroup of a group G . Then the set of cosets of N in G is a group under set composition, called the **quotient group** or **factor group** of G by N and denoted by G/N .

- Set composition of elements of G/N is given by

$$xN \cdot yN = (xy)N \quad \text{for each } x, y \in G.$$

If G is additive, then this is written as

$$(x + N) + (y + N) = (x + y) + N \quad \text{for each } x, y \in G.$$

- The identity of G/N is N .
- For each $x \in G$, the inverse of xN is $x^{-1}N$.

If G is additive, the inverse of $x + N$ is written as $-x + N$.

- If G is finite, then $|G/N| = |G|/|N|$.

You saw earlier that set composition in an abelian group is a commutative binary operation, and set composition in a non-abelian group is a non-commutative binary operation. It follows from the first of these facts that if N is a normal subgroup of an abelian group G , then the quotient group G/N is abelian.

If N is a normal subgroup of a *non-abelian* group G , then the quotient group G/N may be either abelian or non-abelian. This is because even though set composition is not commutative on the set of all *subsets* of G , it may be commutative on the set of all *cosets* of N in G . For example, the group $S(\square)$ is non-abelian but the quotient group $S(\square)/N$, where $N = \{e, b\}$, is abelian, as you can see if you look back at its Cayley table given earlier (for example, after Exercise E54).

As mentioned in the introduction to this unit, you can think of the process of forming a quotient group of a group G as a way of ‘breaking G down’ into two simpler groups N and G/N , just as dividing a natural number by a positive divisor breaks it down into two simpler numbers.

The concept of a quotient group emerged in the second half of the nineteenth century, although it took some time to evolve into the form in which we know it today. Several mathematicians contributed to its development, including Enrico Betti (1823–1892) and Camille Jordan (1838–1922). In addition, it is now known that Richard Dedekind (1831–1916) discovered the concept in the 1850s, but his work was unpublished. Evidence for this surfaced only in the 1970s, so his work had little influence. In 1889 the standard definition of a quotient group appeared in a paper by the German mathematician Otto Hölder (1859–1937) and from then on it began to appear in textbooks and monographs.

The term *factor group* also appears in Hölder’s 1889 paper, though Hölder reserved it for a slightly different notion. The two terms, *quotient group* and *factor group*, were made synonymous in 1897 by the British group theorist William Burnside (1852–1927) after a misreading of Hölder, and both terms are now in common usage with Hölder’s original distinction almost completely lost.



Otto Hölder

It is sometimes possible to observe a quotient group of a finite group in the group table of the original group. If G is a finite group with a normal subgroup N , and we arrange the elements in the row and column headings of the group table of G so that elements in the same coset of N are together, then the quotient group G/N becomes apparent as a ‘blocking’ of the group table.

For example, in the group table for $S(\square)$ on the left in Figure 2, the row and column headings have been arranged so that the elements of each of the cosets

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}$$

of the normal subgroup $N = \{e, b\}$ are together. To highlight the blocking, each coset has been assigned a colour, as indicated by the background colours of the row and column headings, and each element in the table has been given a background colour according to the coset in which it lies. The result is that the body of the table is split into a 4×4 array of 2×2 coloured blocks. Since each colour represents a coset, the coloured blocks form the group table of the quotient group $S(\square)/N$. This quotient group is shown on the right in Figure 2.

| \circ | e | b | a | c | r | t | s | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | b | a | c | r | t | s | u |
| b | b | e | c | a | t | r | u | s |
| a | a | c | b | e | s | u | t | r |
| c | c | a | e | b | u | s | r | t |
| r | r | t | u | s | e | b | c | a |
| t | t | r | s | u | b | e | a | c |
| s | s | u | r | t | a | c | e | b |
| u | u | s | t | r | c | a | b | e |

$S(\square)$

| \cdot | N | aN | rN | sN |
|---------|------|------|------|------|
| N | N | aN | rN | sN |
| aN | aN | N | sN | rN |
| rN | rN | sN | N | aN |
| sN | sN | rN | aN | N |

$S(\square)/N$, where $N = \{e, b\}$

Figure 2 Blocking in the group table of $S(\square)$

Similarly, the group table for \mathbb{Z}_9 on the left in Figure 3 shows the quotient group formed by the cosets of the normal subgroup $\{0, 3, 6\}$. This quotient group is shown on the right in Figure 3.

| $+$ | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 | 8 |
|-----|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 | 8 |
| 3 | 3 | 6 | 0 | 4 | 7 | 1 | 5 | 8 | 2 |
| 6 | 6 | 0 | 3 | 7 | 1 | 4 | 8 | 2 | 5 |
| 1 | 1 | 4 | 7 | 2 | 5 | 8 | 3 | 6 | 0 |
| 4 | 4 | 7 | 1 | 5 | 8 | 2 | 6 | 0 | 3 |
| 7 | 7 | 1 | 4 | 8 | 2 | 5 | 0 | 3 | 6 |
| 2 | 2 | 5 | 8 | 3 | 6 | 0 | 4 | 7 | 1 |
| 5 | 5 | 8 | 2 | 6 | 0 | 3 | 7 | 1 | 4 |
| 8 | 8 | 2 | 5 | 0 | 3 | 6 | 1 | 4 | 7 |

\mathbb{Z}_9

| $+$ | N | $1 + N$ | $2 + N$ |
|---------|---------|---------|---------|
| N | N | $1 + N$ | $2 + N$ |
| $1 + N$ | $1 + N$ | $2 + N$ | N |
| $2 + N$ | $2 + N$ | N | $1 + N$ |

\mathbb{Z}_9/N , where $N = \{0, 3, 6\}$

Figure 3 Blocking in the group table of \mathbb{Z}_9

In contrast, if H is a subgroup that is not normal in a finite group G , and we arrange the elements in the row and column headings of the group table of G so that the elements in the left cosets or right cosets of H are together, then there is no similar blocking effect. For example, in the group table for $S(\square)$ in Figure 4, the row and column headings have been arranged in order of the left cosets of the subgroup $\{e, r\}$ of the group $S(\square)$, which are

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

The resulting coloured blocks, and hence the left cosets, do not form the Cayley table of a group.

| \circ | e | r | a | s | b | t | c | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | r | a | s | b | t | c | u |
| r | r | e | u | c | t | b | s | a |
| a | a | s | b | t | c | u | e | r |
| s | s | a | r | e | u | c | t | b |
| b | b | t | c | u | e | r | a | s |
| t | t | b | s | a | r | e | u | c |
| c | c | u | e | r | a | s | b | t |
| u | u | c | t | b | s | a | r | e |

$S(\square)$

Figure 4 Failure to block in the group table of $S(\square)$

You saw in Unit B1 *Symmetry and groups* that if F is a figure whose symmetry group $S(F)$ is finite and contains indirect symmetries, then the group table of $S(F)$ can be blocked into direct symmetries and indirect symmetries. This is a special case of the blocking into cosets described above, because the direct symmetries form a subgroup $S^+(F)$, which is a normal subgroup since it has index 2 in $S(F)$, and the indirect symmetries form the other coset of $S^+(F)$ in $S(F)$. (Any subgroup of index 2 is normal by Theorem E11 in Unit E1.) For example, Figure 5 shows the group table for $S(\square)$ blocked in this way.

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

$S(\square)$

Figure 5 Blocking of $S(\square)$ into direct symmetries and indirect symmetries

If G is a group with a normal subgroup N , then it can be useful to identify the structure of the quotient group G/N by finding a standard, familiar group to which this quotient group is isomorphic. Here is an example.

Worked Exercise E21

Consider the subgroup $N = \langle 4 \rangle$ of the group U_{15} .

- List the elements of the group U_{15} .
- Find the elements of the subgroup N , and explain why N is normal in U_{15} .
- Find the cosets of N in U_{15} .
- Construct the group table of the quotient group U_{15}/N .
- State the identity element of this quotient group, and state the inverse of each of its elements.
- State a standard group that is isomorphic to this quotient group.

Solution

- The elements of U_{15} are all the numbers in \mathbb{Z}_{15} that are coprime to 15.

We have

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

- The subgroup $N = \langle 4 \rangle$ is the cyclic subgroup of U_{15} generated by 4, so its elements are all the powers of 4 in U_{15} . The binary operation of U_{15} is \times_{15} .

In \mathbb{Z}_{15} we have

$$4^2 = 4 \times_{15} 4 = 1,$$

so 4 has order 2 and hence $N = \langle 4 \rangle = \{1, 4\}$. This subgroup of U_{15} is normal in U_{15} because U_{15} is abelian.

- To find the cosets of N in U_{15} , use Strategy E1 from Unit E1. That is, repeatedly choose an element x of U_{15} not yet assigned to a coset and find the coset containing x , until all the elements of U_{15} have been assigned to cosets.

The cosets are

$$\begin{aligned} N &= \{1, 4\}, \\ 2N &= \{2 \times_{15} 1, 2 \times_{15} 4\} = \{2, 8\}, \\ 7N &= \{7 \times_{15} 1, 7 \times_{15} 4\} = \{7, 13\}, \\ 11N &= \{11 \times_{15} 1, 11 \times_{15} 4\} = \{11, 14\}. \end{aligned}$$

- To find the entries of the group table of U_{15}/N use Theorem E14, which gives

$$xN \cdot yN = (x \times_{15} y)N \quad \text{for all } x, y \in U_{15}.$$

Remember to denote each coset consistently, as one of N , $2N$, $7N$, $11N$. For example,

$$2N \cdot 7N = (2 \times_{15} 7)N = 14N = 11N.$$

The group table of U_{15}/N is as follows.

| \cdot | N | $2N$ | $7N$ | $11N$ |
|---------|-------|-------|-------|-------|
| N | N | $2N$ | $7N$ | $11N$ |
| $2N$ | $2N$ | N | $11N$ | $7N$ |
| $7N$ | $7N$ | $11N$ | N | $2N$ |
| $11N$ | $11N$ | $7N$ | $2N$ | N |

- (e) The identity element of U_{15}/N is N . Each element is self-inverse.
- (f) To find a standard group isomorphic to U_{15}/N , use the table of isomorphism classes near the end of Subsection 3.4 in Unit E1.

The group U_{15}/N has four elements and each element is self-inverse, so it is isomorphic to the Klein four-group V .

Here is a summary of the strategy used in Worked Exercise E21.

Strategy E3

To find a group isomorphic to a finite quotient group G/N where N is a normal subgroup of the group G , do the following.

1. Determine the cosets of N in G , by repeatedly choosing an element x of G not yet assigned to a coset and finding the coset xN (or $x + N$, if G is additive) until all the elements of G have been assigned to cosets.
2. Construct the group table of G/N by composing each pair of cosets using the rule

$$xN \cdot yN = (xy)N$$

(or

$$(x + N) + (y + N) = (x + y) + N$$

if G is additive).

Make sure to use just one way to write each coset.

3. By inspection of the group table, and possibly using the table of isomorphism classes for small groups, identify a standard group isomorphic to G/N .

Exercise E55

Consider the subgroup $N = \langle 4 \rangle$ of \mathbb{Z}_{17}^* .

- Find the elements of N , and explain why it is normal in \mathbb{Z}_{17}^* .
- Find the cosets of N in \mathbb{Z}_{17}^* .
- Construct the group table of the quotient group \mathbb{Z}_{17}^*/N .
- State the identity element of this quotient group, and state the inverse of each of its elements.
- State a standard group that is isomorphic to this quotient group.

Exercise E56

Consider the subgroup $H = \langle 6 \rangle$ of the (additive) group \mathbb{Z}_{12} .

- Find the elements of H , and explain why it is normal in \mathbb{Z}_{12} .
- Find the cosets of N in \mathbb{Z}_{12} .
- Construct the group table of the quotient group \mathbb{Z}_{12}/H .
- State the identity element of this quotient group, and state the inverse of each of its elements.
- State a standard group that is isomorphic to this quotient group.

Exercise E57

The following table is the group table of a group G .

| | e | a | b | c | d | f | g | h |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | d | f | g | h |
| a | a | e | c | b | f | d | h | g |
| b | b | c | e | a | g | h | d | f |
| c | c | b | a | e | h | g | f | d |
| d | d | f | g | h | e | a | b | c |
| f | f | d | h | g | a | e | c | b |
| g | g | h | d | f | b | c | e | a |
| h | h | g | f | d | c | b | a | e |

Consider the subset $N = \{e, a\}$ of G .

- Explain why N is a subgroup of G , and why it is normal in G .
- Find the cosets of N in G .
- Construct the group table of the quotient group G/N .
- State the identity element of this quotient group, and state the inverse of each of its elements.
- State a standard group that is isomorphic to this quotient group.

Exercise E58

The following table is the group table of a group G .

| | e | p | q | r | s | t |
|-----|-----|-----|-----|-----|-----|-----|
| e | e | p | q | r | s | t |
| p | p | e | r | q | t | s |
| q | q | s | e | t | p | r |
| r | r | t | p | s | e | q |
| s | s | q | t | e | r | p |
| t | t | r | s | p | q | e |

Consider the subset $N = \{e, r, s\}$ of G .

- Explain why N is a subgroup of G , and why it is normal in G .
- Find the cosets of N in G .
- Construct the group table of the quotient group G/N .
- State the identity element of this quotient group, and state the inverse of each of its elements.
- State a standard group that is isomorphic to this quotient group.

1.2 Quotient groups of infinite groups

In all the examples of quotient groups G/N in the previous subsection, the group G was finite. In this subsection you will meet some quotient groups G/N where the group G is infinite. In this situation the quotient group G/N may be either finite or infinite, depending on whether the normal subgroup N has finitely many or infinitely many cosets in G .

We will begin by looking at some examples where the normal subgroup has finitely many cosets, so the quotient group is finite. All the examples of this type that we will look at are quotient groups of the infinite additive group $(\mathbb{Z}, +)$, which we will mostly denote simply by \mathbb{Z} .

Quotient groups of $(\mathbb{Z}, +)$

Consider the group \mathbb{Z} . This group is cyclic (it is generated by 1, for example), so all of its subgroups are cyclic, by Theorem B36 in Unit B2 *Subgroups and isomorphisms*. Since it is an additive group, if n is one of its elements then the cyclic subgroup $\langle n \rangle$ generated by n is given by

$$\langle n \rangle = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}.$$

Recall that we denote this subgroup by $n\mathbb{Z}$.

Since \mathbb{Z} is an abelian group, all of its subgroups are normal. So the quotient group $\mathbb{Z}/n\mathbb{Z}$ exists for each integer n .



In the worked exercise below, all the elements of the particular quotient group $\mathbb{Z}/5\mathbb{Z}$ are found; in the exercise that follows you are asked to do the same for $\mathbb{Z}/4\mathbb{Z}$.

Worked Exercise E22

Find all the elements of the quotient group $\mathbb{Z}/5\mathbb{Z}$. Hence state the order of this group.

Solution

The elements of $\mathbb{Z}/5\mathbb{Z}$ are the cosets of $5\mathbb{Z}$ in \mathbb{Z} .

 To find these cosets, we use Strategy E1 from Unit E1: we repeatedly choose an element x of \mathbb{Z} not yet assigned to a coset and find the coset containing x , until all the elements of \mathbb{Z} have been assigned to cosets. 

The cosets are

$$\begin{aligned} 5\mathbb{Z} &= \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}, \\ 1 + 5\mathbb{Z} &= \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}, \\ 2 + 5\mathbb{Z} &= \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\}, \\ 3 + 5\mathbb{Z} &= \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}, \\ 4 + 5\mathbb{Z} &= \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}. \end{aligned}$$

 These five cosets between them contain every element of \mathbb{Z} , so there are no more cosets. 

Hence $\mathbb{Z}/5\mathbb{Z}$ has order 5.

Exercise E59

Find the elements of the quotient group $\mathbb{Z}/4\mathbb{Z}$. Hence state the order of this group.

In the next worked exercise and the exercise that follows we will construct group tables for the quotient groups $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

Worked Exercise E23

Construct a group table for the quotient group $\mathbb{Z}/5\mathbb{Z}$.

Solution

 By Worked Exercise E22, the elements of $\mathbb{Z}/5\mathbb{Z}$ are the five cosets

$$5\mathbb{Z}, \quad 1 + 5\mathbb{Z}, \quad 2 + 5\mathbb{Z}, \quad 3 + 5\mathbb{Z}, \quad 4 + 5\mathbb{Z}.$$

Since \mathbb{Z} is an additive group, the rule for set composition of these cosets is

$$(a + 5\mathbb{Z}) + (b + 5\mathbb{Z}) = (a + b) + 5\mathbb{Z} \quad \text{for all } a, b \in \mathbb{Z}.$$

We make sure to express each coset in the table in just one way, as one of $5\mathbb{Z}$, $1 + 5\mathbb{Z}$, $2 + 5\mathbb{Z}$, $3 + 5\mathbb{Z}$ and $4 + 5\mathbb{Z}$.

For example,

$$(1 + 5\mathbb{Z}) + (2 + 5\mathbb{Z}) = 3 + 5\mathbb{Z},$$

$$(4 + 5\mathbb{Z}) + (2 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z} \quad (\text{since } 6 \in 1 + 5\mathbb{Z}),$$

$$5\mathbb{Z} + (4 + 5\mathbb{Z}) = (0 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 4 + 5\mathbb{Z}.$$

We work out all the composites needed for the table in this way. 

The group table of $\mathbb{Z}/5\mathbb{Z}$ is

| + | $5\mathbb{Z}$ | $1 + 5\mathbb{Z}$ | $2 + 5\mathbb{Z}$ | $3 + 5\mathbb{Z}$ | $4 + 5\mathbb{Z}$ |
|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| $5\mathbb{Z}$ | $5\mathbb{Z}$ | $1 + 5\mathbb{Z}$ | $2 + 5\mathbb{Z}$ | $3 + 5\mathbb{Z}$ | $4 + 5\mathbb{Z}$ |
| $1 + 5\mathbb{Z}$ | $1 + 5\mathbb{Z}$ | $2 + 5\mathbb{Z}$ | $3 + 5\mathbb{Z}$ | $4 + 5\mathbb{Z}$ | $5\mathbb{Z}$ |
| $2 + 5\mathbb{Z}$ | $2 + 5\mathbb{Z}$ | $3 + 5\mathbb{Z}$ | $4 + 5\mathbb{Z}$ | $5\mathbb{Z}$ | $1 + 5\mathbb{Z}$ |
| $3 + 5\mathbb{Z}$ | $3 + 5\mathbb{Z}$ | $4 + 5\mathbb{Z}$ | $5\mathbb{Z}$ | $1 + 5\mathbb{Z}$ | $2 + 5\mathbb{Z}$ |
| $4 + 5\mathbb{Z}$ | $4 + 5\mathbb{Z}$ | $5\mathbb{Z}$ | $1 + 5\mathbb{Z}$ | $2 + 5\mathbb{Z}$ | $3 + 5\mathbb{Z}$ |

Exercise E60

Construct a group table for the quotient group $\mathbb{Z}/4\mathbb{Z}$.

Now look again at the group table for the quotient group $\mathbb{Z}/5\mathbb{Z}$, found in Worked Exercise E23. If we delete every occurrence of ‘ $+ 5\mathbb{Z}$ ’ (writing each occurrence of the coset $5\mathbb{Z}$ as $0 + 5\mathbb{Z}$ before doing so), then we obtain the following table.

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

This is the group table for the group \mathbb{Z}_5 .

This tells us that the quotient group $\mathbb{Z}/5\mathbb{Z}$ is isomorphic to the group \mathbb{Z}_5 , and the following mapping is an isomorphism:

$$\begin{aligned}\phi : \mathbb{Z}/5\mathbb{Z} &\longrightarrow \mathbb{Z}_5 \\ a + 5\mathbb{Z} &\longmapsto a, \quad \text{for } a = 0, 1, 2, 3, 4.\end{aligned}$$

If you look at your answer to Exercise E60, you will see that, similarly, if we delete every occurrence of ‘ $+ 4\mathbb{Z}$ ’ from the group table of the quotient group $\mathbb{Z}/4\mathbb{Z}$ (writing each occurrence of the coset $4\mathbb{Z}$ as $0 + 4\mathbb{Z}$ before doing so), then we obtain the group table for the group \mathbb{Z}_4 . Hence the quotient group $\mathbb{Z}/4\mathbb{Z}$ is isomorphic to the group \mathbb{Z}_4 .

Exercise E61

Write down an isomorphism from the quotient group $\mathbb{Z}/4\mathbb{Z}$ to the group \mathbb{Z}_4 .

In general the theorem below holds. The proof of this theorem is not an important one for you to read: it is a little technical and the general ideas of the proof should be apparent to you from the particular examples $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ above. But read it if you want to see a formal proof.

Theorem E16

For each integer $n \geq 2$, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the group \mathbb{Z}_n , and the following mapping is an isomorphism:

$$\begin{aligned}\phi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}_n \\ a + n\mathbb{Z} &\longmapsto a, \quad \text{for } a = 0, 1, 2, \dots, n-1.\end{aligned}$$

Proof Let n be an integer with $n \geq 2$. First we show that the distinct cosets of $n\mathbb{Z}$ are

$$0 + n\mathbb{Z}, \quad 1 + n\mathbb{Z}, \quad 2 + n\mathbb{Z}, \quad \dots, \quad (n-1) + n\mathbb{Z}.$$

For any elements $a, b \in \mathbb{Z}$, we have

$$\begin{aligned} a + n\mathbb{Z} = b + n\mathbb{Z} &\iff a \in b + n\mathbb{Z} \\ &\iff a = b + nr \quad \text{for some } r \in \mathbb{Z} \\ &\iff a \equiv b \pmod{n}. \end{aligned}$$

That is, two cosets $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ are equal if and only if a and b are congruent modulo n . It follows that the distinct cosets of $n\mathbb{Z}$ in \mathbb{Z} are the n cosets listed above.

Next we show that the mapping ϕ specified in the statement of the theorem is an isomorphism. It follows from what we have just proved that ϕ is one-to-one and onto. It remains to prove that for all $a, b \in \{0, 1, \dots, n-1\}$,

$$\phi((a + n\mathbb{Z}) + (b + n\mathbb{Z})) = \phi(a + n\mathbb{Z}) +_n \phi(b + n\mathbb{Z}).$$

Let $a, b \in \{0, 1, \dots, n-1\}$ and let $c = a +_n b$. Then

$$\begin{aligned} &\phi((a + n\mathbb{Z}) + (b + n\mathbb{Z})) \\ &= \phi((a + b) + n\mathbb{Z}) \quad (\text{by the rule for set composition of cosets of } n\mathbb{Z}) \\ &= \phi(c + n\mathbb{Z}) \quad (\text{since } a + b \equiv c \pmod{n}, \text{ so } (a + b) + n\mathbb{Z} = c + n\mathbb{Z}) \\ &= c \quad (\text{by the rule of } \phi). \end{aligned}$$

Also

$$\begin{aligned} &\phi(a + n\mathbb{Z}) +_n \phi(b + n\mathbb{Z}) \\ &= a +_n b \quad (\text{by the rule of } \phi) \\ &= c. \end{aligned}$$

Hence the required equation holds. This completes the proof. ■

We can use Theorem E16 to deduce facts about a quotient group $\mathbb{Z}/n\mathbb{Z}$ from facts that we know about the group \mathbb{Z}_n . For example, since \mathbb{Z}_n is a cyclic group of order n , Theorem E16 tells us that the quotient group $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n .

You are asked to use Theorem E16 in this way in the next exercise. You will need to use the result that if $\phi : (G, \circ) \rightarrow (H, *)$ is an isomorphism, then g is a generator of (G, \circ) if and only if $\phi(g)$ is a generator of $(H, *)$. This follows from Theorem B46 in Unit B2, which states that if $\phi : (G, \circ) \rightarrow (H, *)$ is an isomorphism, then an element $g \in (G, \circ)$ and its image $\phi(g) \in (H, *)$ either both have the same finite order or both have infinite order. Remember that the generators of \mathbb{Z}_n are the integers in \mathbb{Z}_n that are coprime to n . (See Corollary B40 in Unit B2.)

Exercise E62

Find all the generators of each of the following quotient groups.

- (a) $\mathbb{Z}/6\mathbb{Z}$ (b) $\mathbb{Z}/4\mathbb{Z}$ (c) $\mathbb{Z}/5\mathbb{Z}$

The quotient group \mathbb{R}/\mathbb{Z}

We now consider an example of a quotient group G/N for which not only is G an infinite group, but also G/N is an infinite group. In other words, the normal subgroup N has infinitely many cosets in G . We will look at just a single example of such a quotient group here, namely the quotient group \mathbb{R}/\mathbb{Z} , where \mathbb{R} and \mathbb{Z} denote the additive groups $(\mathbb{R}, +)$ and $(\mathbb{Z}, +)$.

The quotient group \mathbb{R}/\mathbb{Z} certainly exists, because \mathbb{R} is an abelian group, and hence its subgroup \mathbb{Z} is normal.

The elements of the quotient group \mathbb{R}/\mathbb{Z} are the cosets of \mathbb{Z} in \mathbb{R} . For any real number $x \in \mathbb{R}$, the coset to which x belongs is

$$\begin{aligned} x + \mathbb{Z} &= x + \{\dots, -2, -1, 0, 1, 2, \dots\}, \\ &= \{\dots, x - 2, x - 1, x, x + 1, x + 2, \dots\}. \end{aligned}$$

Here are some examples of such cosets:

$$\begin{aligned} 1 + \mathbb{Z} &= \{\dots, 1 - 2, 1 - 1, 1, 1 + 1, 1 + 2, \dots\} \\ &= \{\dots, -1, 0, 1, 2, 3, \dots\} \\ &= \mathbb{Z}, \\ 1.6 + \mathbb{Z} &= \{\dots, 1.6 - 2, 1.6 - 1, 1.6, 1.6 + 1, 1.6 + 2, \dots\} \\ &= \{\dots, -0.4, 0.6, 1.6, 2.6, 3.6, \dots\}, \\ 2.6 + \mathbb{Z} &= \{\dots, 2.6 - 2, 2.6 - 1, 2.6, 2.6 + 1, 2.6 + 2, \dots\} \\ &= \{\dots, 0.6, 1.6, 2.6, 3.6, 4.6, \dots\}. \end{aligned}$$

Of course, different values of x can give the same coset $x + \mathbb{Z}$. For instance, the examples above show that

$$1.6 + \mathbb{Z} = 2.6 + \mathbb{Z}.$$

Exercise E63

Consider the following list of five cosets of \mathbb{Z} in \mathbb{R} :

$$0.2 + \mathbb{Z}, \quad 1.2 + \mathbb{Z}, \quad 3.7 + \mathbb{Z}, \quad -1.3 + \mathbb{Z}, \quad -4.8 + \mathbb{Z}.$$

- Find each of these cosets. (As in the examples above, list enough elements of each coset to make the full infinite list of elements clear.)
- How many different cosets are there in the list?

To help us understand the structure of \mathbb{R}/\mathbb{Z} , it is useful to express each coset of \mathbb{Z} in \mathbb{R} in a single, consistent way, just as we did for the cosets in each quotient group that we considered earlier.

To see how we might do this, observe that each coset $x + \mathbb{Z}$ of \mathbb{Z} in \mathbb{R} consists of the set \mathbb{Z} shifted (by x) along the real line, as illustrated in Figure 6.

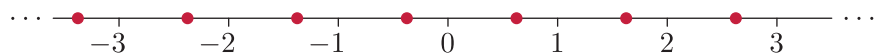


Figure 6 The elements of a coset $x + \mathbb{Z}$

Thus each coset contains exactly one real number in the interval $[0, 1)$.

For example, the coset $1.2 + \mathbb{Z}$, shown in Figure 7, contains the real number $0.2 \in [0, 1)$.

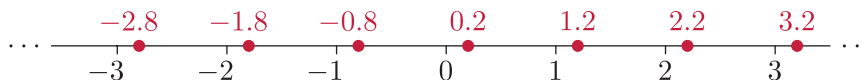


Figure 7 The elements of the coset $1.2 + \mathbb{Z}$

Similarly, the coset $-1.3 + \mathbb{Z}$, shown in Figure 8, contains the real number $0.7 \in [0, 1)$.

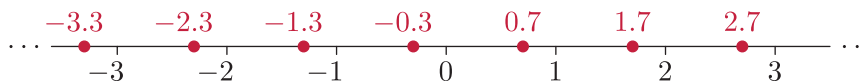


Figure 8 The elements of the coset $-1.3 + \mathbb{Z}$

This gives us a way to write each coset of \mathbb{Z} in \mathbb{R} in a single, consistent way: we write it in the form $x + \mathbb{Z}$ where $x \in [0, 1)$. For example, we write the coset $1.2 + \mathbb{Z}$ as $0.2 + \mathbb{Z}$, and the coset $-1.3 + \mathbb{Z}$ as $0.7 + \mathbb{Z}$, and so on.

Exercise E64

Write each of the following cosets of \mathbb{Z} in \mathbb{R} in the form $x + \mathbb{Z}$ where $x \in [0, 1)$.

- (a) $3.1 + \mathbb{Z}$ (b) $-0.22 + \mathbb{Z}$ (c) $-3.1 + \mathbb{Z}$

Notice that to express a coset $y + \mathbb{Z}$ of \mathbb{Z} in \mathbb{R} in the form $x + \mathbb{Z}$ where $x \in [0, 1)$ we take $x = \text{frac}(y)$, where $\text{frac}(y)$ is the *fractional part* of y . Remember from Unit E1 that the **fractional part** $\text{frac}(x)$ of a real number x is given by

$$\text{frac}(x) = x - \lfloor x \rfloor,$$

where $\lfloor x \rfloor$ is the integer part of x (the largest integer that is less than or equal to x). Essentially, $\text{frac}(x)$ is equal to 0 if x is an integer, and is equal to the distance from x to ‘the next integer down’ otherwise, as illustrated in Figure 9.

For example, we write

$$1.2 + \mathbb{Z} \text{ as } 0.2 + \mathbb{Z} \text{ because } \text{frac}(1.2) = 0.2,$$

$$-1.3 + \mathbb{Z} \text{ as } 0.7 + \mathbb{Z} \text{ because } \text{frac}(-1.3) = 0.7,$$

$$1 + \mathbb{Z} \text{ as } 0 + \mathbb{Z} = \mathbb{Z} \text{ because } \text{frac}(1) = 0.$$

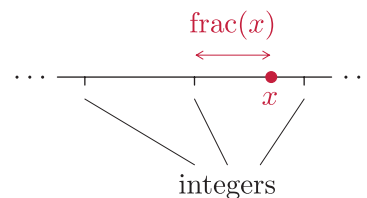


Figure 9 The fractional part of a real number x

We now have a helpful way to express the elements of the quotient group \mathbb{R}/\mathbb{Z} , so we turn to looking at how these elements are composed in \mathbb{R}/\mathbb{Z} . They are cosets, so we compose them using set composition. Since \mathbb{R} is an additive group, the rule for set composition of cosets of \mathbb{Z} in \mathbb{R} is

$$(x + \mathbb{Z}) + (y + \mathbb{Z}) = (x + y) + \mathbb{Z}.$$

We make sure to express each composite in the form $x + \mathbb{Z}$ where $x \in [0, 1)$.

For example,

$$\begin{aligned}(0.25 + \mathbb{Z}) + (0.7 + \mathbb{Z}) &= 0.95 + \mathbb{Z}, \\ (0.3 + \mathbb{Z}) + (0.96 + \mathbb{Z}) &= 1.26 + \mathbb{Z} = 0.26 + \mathbb{Z}.\end{aligned}$$

Consider the effect of deleting the occurrences of ‘ $+ \mathbb{Z}$ ’ in the calculations above (and replacing the symbol $+$ for set composition with the words ‘composed with’):

$$\begin{aligned}0.25 \text{ composed with } 0.7 &= 0.95, \\ 0.3 \text{ composed with } 0.96 &= 0.26.\end{aligned}\tag{1}$$

These calculations may remind you of calculations involving the binary operation $+_1$, which you met in Subsection 1.1 of Unit E1. Recall that this binary operation is defined on the interval $[0, 1)$ by

$$x +_1 y = \text{frac}(x + y).$$

So, for example,

$$\begin{aligned}0.25 +_1 0.7 &= 0.95, \\ 0.3 +_1 0.96 &= 0.26.\end{aligned}\tag{2}$$

Equations (1) and equations (2) illustrate the fact that to compose two elements $x + \mathbb{Z}$ and $y + \mathbb{Z}$ of \mathbb{R}/\mathbb{Z} , where $x, y \in [0, 1)$, we compose the numbers x and y using the binary operation $+_1$.

Exercise E65

Determine the following composites of cosets in the group \mathbb{R}/\mathbb{Z} .

- (a) $(0.9 + \mathbb{Z}) + (0.8 + \mathbb{Z})$ (b) $(0.2 + \mathbb{Z}) + \mathbb{Z}$
- (c) $(0.5 + \mathbb{Z}) + (0.7 + \mathbb{Z}) + (0.8 + \mathbb{Z})$

You might remember that the interval $[0, 1)$ is a group under the binary operation $+_1$: you were asked to prove this in Exercise E2 in Subsection 1.1 of Unit E1.

You have now seen that every element of \mathbb{R}/\mathbb{Z} corresponds to a unique element of the interval $[0, 1)$, and that to compose two elements of \mathbb{R}/\mathbb{Z} we compose the corresponding two elements of $[0, 1)$ using the binary operation $+_1$. This tells us that the group $(\mathbb{R}/\mathbb{Z}, +)$ is isomorphic to the group $([0, 1), +_1)$, as stated in the theorem below. The proof of this

theorem is not an important proof for you to read: as with the proof of Theorem E16, the general ideas of the proof should be apparent from the discussion above.

Theorem E17

The quotient group \mathbb{R}/\mathbb{Z} is isomorphic to the group $([0, 1), +_1)$, and the following mapping is an isomorphism:

$$\begin{aligned}\phi : \mathbb{R}/\mathbb{Z} &\longrightarrow [0, 1) \\ x + \mathbb{Z} &\longmapsto x, \quad \text{for } x \in [0, 1).\end{aligned}$$

Proof We have seen that the distinct cosets of \mathbb{Z} in \mathbb{R} are given by

$$x + \mathbb{Z} \quad \text{where } x \in [0, 1).$$

It follows that the mapping specified in the statement of the theorem is one-to-one and onto. It remains to prove that for all $x, y \in [0, 1)$,

$$\phi((x + \mathbb{Z}) + (y + \mathbb{Z})) = \phi(x + \mathbb{Z}) +_1 \phi(y + \mathbb{Z}).$$

Let $x, y \in [0, 1)$ and let $z = x +_1 y$. Then

$$\begin{aligned}\phi((x + \mathbb{Z}) + (y + \mathbb{Z})) &= \phi((x + y) + \mathbb{Z}) \quad (\text{by the rule for set composition of cosets of } \mathbb{Z} \text{ in } \mathbb{R}) \\ &= \phi(z + \mathbb{Z}) \quad (\text{since } x +_1 y = z, \text{ so } (x + y) + \mathbb{Z} = z + \mathbb{Z}) \\ &= z \quad (\text{by the rule of } \phi),\end{aligned}$$

and

$$\begin{aligned}\phi(x + \mathbb{Z}) +_1 \phi(y + \mathbb{Z}) &= x +_1 y \quad (\text{by the rule of } \phi) \\ &= z.\end{aligned}$$

Hence the required equation holds. This completes the proof. ■

In the next exercise you might find it helpful to use Theorem E17 along with the fact that if $\phi : (G, \circ) \longrightarrow (H, *)$ is an isomorphism then an element $g \in (G, \circ)$ and its image $\phi(g) \in (H, *)$ either both have the same finite order or both have infinite order (Theorem B46 from Unit B2).

Exercise E66

- (a) Find the order of the element $0.25 + \mathbb{Z}$ of \mathbb{R}/\mathbb{Z} , and write down the elements of the cyclic subgroup generated by this element.
- (b) For each of the following possible orders of elements of \mathbb{R}/\mathbb{Z} , write down an element of \mathbb{R}/\mathbb{Z} with that order.
 - (i) 5 (ii) 2 (iii) 3 (iv) 1

1.3 Simple groups (optional)

In this optional subsection you can learn about the idea of a *simple group*, which is extremely important in advanced group theory.

You have seen that every group of order 2 or more has at least two normal subgroups, namely itself and its trivial subgroup $\{e\}$. A group of order 2 or more that has no normal subgroups other than these two is called a simple group.

Definition

A group G of order 2 or more is **simple** if it has no proper non-trivial normal subgroups.

If G is a simple group, then the only quotient groups of G are

- the group $G/\{e\}$, which is isomorphic to G (because each coset of $\{e\}$ in G contains only one element)
- the group G/G , which is isomorphic to $\{e\}$ (because the only coset of G in G is G itself, which is the identity element of G/G).

As you saw in Subsection 1.1, we can think of the process of forming the quotient group of a group G by a normal subgroup N as a way of ‘breaking down’ G into the two simpler groups N and G/N , just as dividing a natural number by a positive divisor breaks it down into two ‘simpler’ numbers. But if G is simple, then we *cannot* break it down into simpler groups in this way – if we try, then the only groups that we obtain are the group $\{e\}$ and G itself.

If we pursue the analogy with the natural numbers, then the simple groups are rather like the prime numbers, whose only positive divisors are 1 and the number itself. Moreover, just as the prime numbers are the basic building blocks of the natural numbers, so the simple groups can be thought of as the basic building blocks of all groups. For this reason, it is of considerable importance in group theory to know which groups are simple. Both finite and infinite groups can be simple, but here we will consider only finite simple groups.

Here is an exercise to get you thinking about which finite groups might be simple.

Exercise E67

Determine whether the following groups are simple. (The non-identity elements of $S(\square)$ are shown in Figure 10.)

- (a) $S(\square)$ (b) \mathbb{Z}_6 (c) \mathbb{Z}_7

It turns out to be relatively straightforward to show which finite *abelian* groups are simple. You saw examples that illustrate the next result in Exercise E67(b) and (c).

Theorem E18

Let G be a finite abelian group. Then G is simple if and only if it is a cyclic group of prime order.

Proof**‘If’ part**

Suppose that G is a cyclic group of prime order, p say. Then, by Lagrange’s Theorem, the order of any subgroup of G is either 1 or p . It follows that the only subgroups of G are $\{e\}$ and G , so G is simple.

‘Only if’ part

Suppose that G is simple. Then the order of G is at least 2. Let x be any element of G other than the identity element. Since G is abelian, the cyclic subgroup $\langle x \rangle$ generated by x is normal in G , by Theorem E10 in Unit E1. Since G is simple it follows that $\langle x \rangle = G$, so G is cyclic.

Now suppose that the order n of the element x (and hence the order of G) is a *not* a prime number. Then $n = rs$, say, where r and s are integers such that $1 < r, s < n$. It follows that the element x^r has order s , because

$$(x^r)^s = x^{rs} = x^n = e$$

whereas if t is an integer such that $1 \leq t < s$ then

$$(x^r)^t \neq e,$$

because otherwise we would have $x^{rt} = e$, which is not true because x has order n and $1 < rt < rs = n$. Thus the cyclic subgroup $\langle x^r \rangle$ generated by x^r has order s . Since $1 < s < n$, this shows that $\langle x^r \rangle$ is a proper non-trivial normal subgroup of G , which is a contradiction because G is simple. It follows that G is a cyclic group of prime order. ■

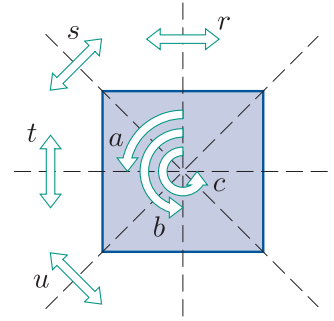


Figure 10 $S(\square)$

Theorem E18 gives a complete answer to the question ‘Which finite abelian groups are simple?’ Let us now briefly consider some finite *non-abelian* groups.

You have met several standard families of such groups, as follows.

- The symmetry groups of regular polygons, such as $S(\triangle)$, $S(\square)$, $S(\diamond)$, and so on, which are all non-abelian. These groups are called the *dihedral groups* of orders 6, 8, 10, and so on.
- The symmetric groups S_n , which are non-abelian for $n \geq 3$.
- The alternating groups A_n , which are non-abelian for $n \geq 4$.

It is straightforward to check that all these groups *are* non-abelian, as follows. In a dihedral group $S(F)$ where F is a regular polygon any two reflections x and y in adjacent axes of symmetry satisfy $xy \neq yx$. Also, for any $n \geq 4$, the permutations $(1\ 2\ 3)$ and $(2\ 3\ 4)$ are elements of both S_n and A_n , and $(1\ 2\ 3)(2\ 3\ 4) = (1\ 2)(3\ 4)$ whereas $(2\ 3\ 4)(1\ 2\ 3) = (1\ 3)(2\ 4)$. The group S_3 is isomorphic to $S(\triangle)$ and is therefore non-abelian.

Each dihedral group $S(F)$ where F is a regular polygon is not simple, because its subgroup $S^+(F)$ of direct symmetries has index 2 in $S(F)$ and is therefore normal in $S(F)$. Similarly, each symmetric group S_n with $n \geq 3$ is not simple, because its subgroup A_n has index 2 in S_n and is therefore normal in S_n (as stated in Corollary E12 in Unit E1).

The first non-abelian alternating group, A_4 , is not simple either, because, as you saw in Exercise E47 in Section 5 of Unit E1, its subgroup

$$K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

is a normal subgroup. However, the next alternating group, A_5 , *is* simple, as is shown in the solution to Exercise E88 in Subsection 3.3 later in this unit.

In fact it can be shown that the alternating group A_5 , which has order 60, is the *smallest* non-abelian simple group, and that in general the following theorem holds. This theorem was originally proved by Évariste Galois (see the blue box below).

Theorem E19

The alternating group A_n is simple for $n \geq 5$.

It turns out that answering the question ‘Which finite non-abelian groups are simple?’ is a vastly difficult task. You can read a little about its history in the boxes below.

Simple groups and polynomial equations

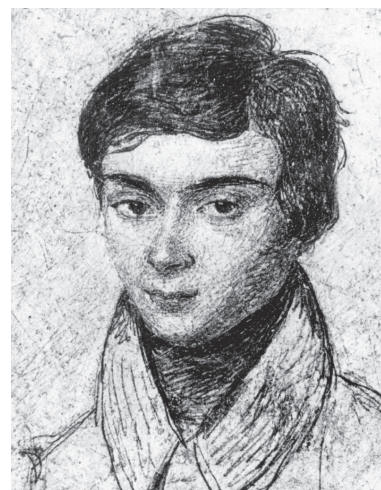
In 1799 the Italian mathematician Paolo Ruffini (1765–1822), building on earlier work of Lagrange on permutations, asserted and almost proved that the general quintic equation cannot be solved by radicals (in other words, there is no formula in terms of roots for the solutions of a polynomial equation of degree 5). The proof was completed by Niels Henrik Abel (1802–1829), who published it in 1824, with a longer, more detailed version in 1826.

Abel gave no criterion for distinguishing between polynomial equations that can be solved by radicals (such as $(x - 1)^5 = 0$) and those that cannot. This issue was resolved by Évariste Galois (1811–1832), in a memoir written in 1830 when he was still a teenager but only published posthumously in 1846 (he died at the age of 20 following a duel). Galois showed that whether or not a polynomial equation is solvable by radicals is equivalent to whether or not a particular permutation group formed by its solutions has a certain structure. Fundamental for his resolution of the problem was his proof of the result that, in modern language, the alternating group A_n is simple for $n \geq 5$.

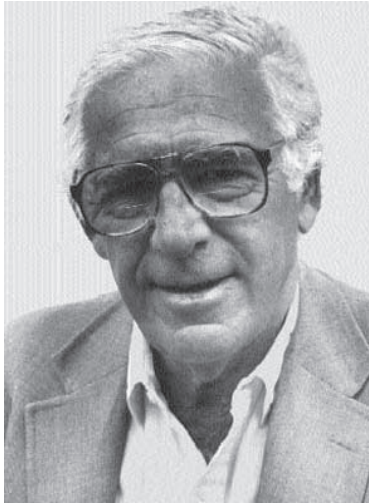
Galois’ work was notoriously difficult for his contemporaries to understand and it took many decades before it was recast in the form in which it is studied today. For example, the term ‘alternating group’ was not used until 1873, when it appeared in an article by Camille Jordan.



Niels Henrik Abel



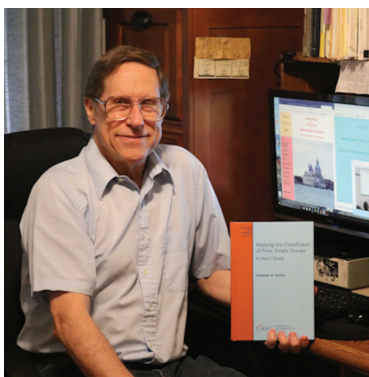
Évariste Galois



Daniel Gorenstein



Michael Aschbacher



Stephen Smith

The classification of finite simple groups

Given the importance of finite simple groups – they can be thought of as the building blocks of all finite groups – it was natural for mathematicians to want to classify them. This led to a monumental collective effort that began in the nineteenth century and gathered pace in the second half of the twentieth century. About a hundred mathematicians were involved, and together they published several hundred journal articles covering tens of thousands of pages. Much of the work was overseen by Daniel Gorenstein (1923–1982) who said in 1979 that ‘it makes more sense to view this classification as an entire field of mathematics rather than as an attempt to prove a single theorem’. Gorenstein announced in February 1981 that the classification was complete, but in fact the final gap in the proof was closed in 2004 by Michael Aschbacher (1944–) and Stephen Smith (1948–). The resulting theorem, one of the most extraordinary in pure mathematics, can be summarised as follows.

Classification theorem for finite simple groups

Let G be a finite simple group. Then G lies in one (or more) of the following families:

- the cyclic groups of prime order
- the alternating groups of degree at least 5
- the finite groups of Lie type (these groups are beyond the scope of this module)
- 26 groups known as the *sporadic groups*.

So apart from the 26 sporadic groups, all finite simple groups fit into patterns. The largest sporadic group is known as the *Monster*: it has order

$$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \\ \times 47 \times 59 \times 71,$$

which is approximately equal to 8×10^{53} .

The classification theorem is an enormously powerful result: many problems in group theory can be reduced to problems about simple groups or groups closely related to simple groups, allowing knowledge about simple groups to be used to solve them. By 2004 almost none of the major problems in finite group theory that were unsolved before 1980 remained open. However, the classification theorem has not ended research into finite groups, in much the same way that the discovery of the periodic table did not stop research in chemistry.

(Source: Gorenstein, D. (1979) ‘The classification of finite simple groups 1. Simple groups and local analysis’, *Bulletin of the American Mathematical Society* vol. 1, no. 1, pp. 43–199.)

2 Conjugacy

In this section you will start by revising the idea of *conjugacy* in symmetric groups, which you studied in Unit B3. Then you will see how this idea can be generalised to all groups. The idea of conjugacy is related to the existence of normal subgroups, and hence to the ability to construct quotient groups, as you will see in Section 3.

2.1 Conjugacy in symmetric groups

Remember that for each positive integer n the symmetric group S_n is the group of all permutations of the set $\{1, 2, \dots, n\}$.

You met the following definition in Subsection 4.1 of Unit B3.

Definition

Let x and y be permutations in S_n . We say that y is a **conjugate** of x in S_n if there is a permutation g in S_n such that

$$y = g \circ x \circ g^{-1}.$$

We also say that:

- g **conjugates** x to y
- y is the **conjugate** of x by g
- g is a **conjugating permutation**.

For example, the permutation $(2\ 3\ 5)(4\ 6)$ is a conjugate of the permutation $(1\ 4\ 3)(2\ 6)$ in S_6 because $(1\ 3\ 2\ 4\ 5) \in S_6$ and

$$(2\ 3\ 5)(4\ 6) = (1\ 3\ 2\ 4\ 5) \circ (1\ 4\ 3)(2\ 6) \circ (1\ 3\ 2\ 4\ 5)^{-1}, \quad (3)$$

as we will check shortly. This equation shows that $(1\ 3\ 2\ 4\ 5)$ conjugates $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$.

To check equation (3), we have to simplify the expression on the right-hand side. That is, we have to find the conjugate of $(1\ 4\ 3)(2\ 6)$ by $(1\ 3\ 2\ 4\ 5)$. One way to do this is to find the inverse of the permutation $(1\ 3\ 2\ 4\ 5)$, then compose the three permutations in the usual way. However, there is a much quicker way to find conjugates in a symmetric group, as follows.

Strategy E4 Renaming method

To find the conjugate $g \circ x \circ g^{-1}$, where x and g are permutations in S_n , replace each symbol in the cycle form of x by its image under g .



We refer to this strategy as the ‘renaming method’ because it involves ‘renaming’ each symbol in a permutation x using the conjugating permutation g . The reason why it works is explained shortly, but first here is a worked exercise to demonstrate it, and an exercise in which you can practise it.

Worked Exercise E24

Use the renaming method, Strategy E4, to find the conjugate

$$(1\ 3\ 2\ 4\ 5) \circ (1\ 4\ 3)(2\ 6) \circ (1\ 3\ 2\ 4\ 5)^{-1}.$$

Solution

 Rename the symbols in $(1\ 4\ 3)(2\ 6)$ using $(1\ 3\ 2\ 4\ 5)$: that is, replace each symbol in $(1\ 4\ 3)(2\ 6)$ by its image under $(1\ 3\ 2\ 4\ 5)$. 

We have

$$\begin{array}{ccccccc} & & (1\ 4\ 3)(2\ 6) & & & & \\ (1\ 3\ 2\ 4\ 5) & \downarrow\downarrow\downarrow & \downarrow\downarrow & & & & \\ & & (3\ 5\ 2)(4\ 6) & = & (2\ 3\ 5)(4\ 6). & & \end{array}$$

Thus

$$(1\ 3\ 2\ 4\ 5) \circ (1\ 4\ 3)(2\ 6) \circ (1\ 3\ 2\ 4\ 5)^{-1} = (2\ 3\ 5)(4\ 6).$$

Worked Exercise E24 confirms that $(1\ 3\ 2\ 4\ 5)$ conjugates $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$, as claimed by equation (3).

Exercise E68

- (a) Use the renaming method, Strategy E4, to find the following conjugates in S_5 .
- (i) $(1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (1\ 3\ 5)^{-1}$
 - (ii) $(1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ ((1\ 3)(2\ 4\ 5))^{-1}$
- (b) Check your answers to part (a) by finding the inverse of $(1\ 3\ 5)$ and the inverse of $(1\ 3)(2\ 4\ 5)$ and composing the permutations in the usual way.

To see why the renaming method, Strategy E4, works consider the example of the permutations

$$x = (1\ 4\ 3)(2\ 6) \quad \text{and} \quad g = (1\ 3\ 2\ 4\ 5)$$

in S_6 , from Worked Exercise E24. Let y be the permutation obtained by renaming the symbols in x using g , as shown below.

$$\begin{array}{ccccccc} & & x = (1\ 4\ 3)(2\ 6) & & & & \\ (1\ 3\ 2\ 4\ 5) = g & \downarrow & \downarrow\downarrow\downarrow & \downarrow\downarrow & & & \\ & & y = (3\ 5\ 2)(4\ 6) & & & & \end{array} \tag{4}$$

Strategy E4 claims that y is equal to $g \circ x \circ g^{-1}$. Here is an explanation of why this is.

Let us focus on one particular symbol in the set $\{1, 2, 3, 4, 5, 6\}$, say 3, and find its image under y . We can see immediately from the cycle form of y found above that the image of 3 under y is 5. Let us find the image of 3 under y in another way, namely by using the cycle form of x , since y is just x with the symbols renamed. We proceed as follows. We first find the symbol that was renamed as 3. To do this, we go backwards along the arrow that points to the symbol 3 in diagram (4) above. That is, we find the image of 3 under the permutation g^{-1} . This gives the symbol 1. Then we use the cycle form of x to find the image of 1 under x . This gives 4. Finally, we find the symbol that is the new name of the symbol 4. That is, we find the image of 4 under the permutation g . This gives 5. So we have found in another way that the image of 3 under y is 5.

The process described above shows that the effect of applying the permutation y to the symbol 3 is the same as the effect of applying the permutation g^{-1} , then the permutation x , then the permutation g to the symbol 3, as illustrated in Figure 11. That is, the two permutations y and $g \circ x \circ g^{-1}$ have the same effect on the symbol 3. There is nothing special about the symbol 3 here, of course: the same will be true for any symbol in the set $\{1, 2, 3, 4, 5, 6\}$. In other words, the permutations y and $g \circ x \circ g^{-1}$ are equal, as claimed.

The ideas above hold whenever we use a permutation g to rename the symbols in a permutation x : the permutation that we obtain is equal to $g \circ x \circ g^{-1}$. This explains why Strategy E4 works.

Notice that the equation

$$y = g \circ x \circ g^{-1}$$

in the definition of a conjugate can be rearranged as

$$g^{-1} \circ y \circ g = x$$

(by composing both sides of the original equation on the left by g^{-1} and on the right by g). The rearranged equation can be written as

$$x = g^{-1} \circ y \circ (g^{-1})^{-1}.$$

Thus if g conjugates x to y , then g^{-1} conjugates y to x . This makes sense in view of Strategy E4, because if renaming the symbols in x using g gives y , then of course renaming the symbols in y using g^{-1} gives x .

So if y is a conjugate of x in S_n , then x is a conjugate of y in S_n , and we can simply say that x and y are **conjugates** or **conjugate permutations** in S_n , or that they are **conjugate** in S_n . These are all ways of saying that each of x and y is a conjugate of the other in S_n .

Since renaming the symbols in a permutation does not change its cycle structure, permutations that are conjugate in S_n always have the same cycle structure.

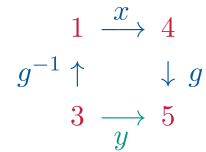


Figure 11 The image of the symbol 3 under the permutation y , found in two different ways

It is also true that any two permutations in S_n with the same cycle structure are conjugate in S_n . This is because if two permutations x and y in S_n have the same cycle structure, then there is always at least one permutation g in S_n that conjugates x to y ; it can be found by using the following strategy, which you met in Unit B3.

Strategy B12

To find a permutation g such that $y = g \circ x \circ g^{-1}$, where x and y are permutations with the same cycle structure, do the following.

Use the fact that g renames x to y , as follows.

1. Match up the cycles of x and y (including 1-cycles) so that cycles of equal lengths correspond.



$$\begin{array}{ccccccc} x & = & (*) & * & \cdots & * &)(*) & * & \cdots & * &) \cdots (*) & (*) \\ g & \downarrow & & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\ y & = & (*) & * & \cdots & * &)(*) & * & \cdots & * &) \cdots (*) & (*) \end{array}$$

2. Read off the two-line form of the renaming permutation g from this diagram. Usually, write g in cycle form.

Worked Exercise E25



- (a) Use Strategy B12 to find a permutation g in S_6 that conjugates $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$.
- (b) Find another permutation g in S_6 that does this.

Solution

- (a)  Write the cycle form of $(2\ 3\ 5)(4\ 6)$ underneath the cycle form of $(1\ 4\ 3)(2\ 6)$, matching up cycles of the same length, and including the 1-cycles. 

We can write

$$\begin{array}{ccccccc} & (1\ 4\ 3)(2\ 6)(5) \\ g & \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \\ & (2\ 3\ 5)(4\ 6)(1). \end{array}$$

 Interpret this diagram as the two-line form of a conjugating permutation g , and write down the cycle form of g . The permutation g maps 1 to 2, so it has a cycle starting $(1\ 2\ \cdots)$. It maps 2 to 4, so the cycle continues $(1\ 2\ 4\ \cdots)$. We continue in this way to find the cycle form of g . 

A conjugating permutation g is

$$g = (1\ 2\ 4\ 3\ 5)(6) = (1\ 2\ 4\ 3\ 5).$$

- (b) There are several alternative ways to match up the cycles in the permutations $(2\ 3\ 5)(4\ 6)$ and $(1\ 4\ 3)(2\ 6)$, because the starting numbers in the cycles can be changed.

Another conjugating permutation g is given by

$$g \begin{array}{ccccccc} (1\ 4\ 3)(2\ 6)(5) \\ \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \\ (5\ 2\ 3)(4\ 6)(1). \end{array}$$

This gives

$$g = (1\ 5)(3)(2\ 4)(6) = (1\ 5)(2\ 4).$$

Exercise E69

There are six permutations in S_6 that conjugate $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$. One of these, $(1\ 3\ 2\ 4\ 5)$, was given in Worked Exercise E24, and another two, $(1\ 2\ 4\ 3\ 5)$ and $(1\ 5)(2\ 4)$, were found in Worked Exercise E25. Determine the other three permutations.

Exercise E70

Find all the permutations in S_4 that conjugate $(1\ 3)$ to $(3\ 4)$.

The discussion in this subsection justifies the following theorem, which you met in Unit B3.

Theorem B64

Two permutations in the symmetric group S_n are conjugate in S_n if and only if they have the same cycle structure.

Since the order of a permutation depends only on its cycle structure, it follows from Theorem B64 that permutations that are conjugate in S_n always have the same order.

2.2 Conjugacy in general

So far you have seen the idea of conjugacy applied only to symmetric groups. We will now extend the idea of conjugacy to all groups. We make the following definition.

Definition

Let x and y be elements of a group G . We say that y is a **conjugate** of x in G if there exists an element g in G such that

$$y = gxg^{-1}.$$

We also say that

- g **conjugates** x to y
- y is the **conjugate** of x by g
- g is a **conjugating element**.

This definition is written using concise multiplicative notation for a general group G , in the usual way. If the binary operation of a particular group G is denoted by \circ , for example, then as you would expect we write a conjugate in G in the form $g \circ x \circ g^{-1}$ rather than gxg^{-1} . For example, this applies to symmetric groups and symmetry groups.

Worked Exercise E26

Find the conjugate $r \circ a \circ r^{-1}$ in the group $S(\triangle)$.

(The non-identity symmetries of the equilateral triangle are shown in Figure 12 and the group table of $S(\triangle)$ is given as Table 5.)

Solution

$$r \circ a \circ r^{-1} = r \circ a \circ r = r \circ (a \circ r) = r \circ t = b$$

Exercise E71

Find the following conjugates in the group $S(\triangle)$.

- (a) $s \circ a \circ s^{-1}$ (b) $a \circ a \circ a^{-1}$ (c) $e \circ a \circ e^{-1}$ (d) $b \circ a \circ b^{-1}$

Exercise E72

Let G be an abelian group and let $x \in G$. Show that for all $g \in G$ the conjugate of x by g is equal to x .

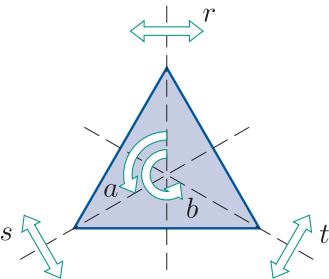


Figure 12 The symmetries of the equilateral triangle

Table 5 $S(\triangle)$

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

Exercise E72 shows that in an abelian group the only conjugate of an element x is x itself. So conjugacy in an abelian group is rather boring! In a non-abelian group, a conjugate of an element x may be x itself or it may be a different element, as illustrated by Worked Exercise E26 and Exercise E71 above.

Exercise E73

Let G be a group with identity e and let $x \in G$.

- (a) Show that the conjugate of e by x is equal to e .
- (b) Show that the conjugate of x by e is equal to x .

Exercise E73(a) shows that in any group the only conjugate of the identity element e is itself. Exercise E73(b) shows that in any group every element is a conjugate of itself.

In the previous subsection you saw that, in a symmetric group S_n , if a permutation y is a conjugate of a permutation x , then x is also a conjugate of y . This property extends to conjugates in any group: if y is a conjugate of x in the group, then x is also a conjugate of y in the group. The justification of this is the same as for conjugates in S_n : the equation

$$y = gxg^{-1}$$

in the definition of a conjugate can be rearranged as

$$g^{-1}yg = x$$

(by composing both sides of the original equation on the left by g^{-1} and on the right by g), and the rearranged equation can be written as

$$x = g^{-1}y(g^{-1})^{-1}.$$

This shows that if g conjugates x to y , then g^{-1} conjugates y to x . Because of this, instead of saying that y is a conjugate of x in a group G , we can simply say that x and y are **conjugates** or **conjugate elements** in G , or that they are **conjugate** in G . These are all ways of saying that each of x and y is a conjugate of the other in G .

There is another useful property of conjugacy in symmetric groups that extends to any group. You saw in the previous subsection that conjugate permutations have the same cycle structure, and therefore have the same order. In fact, conjugate elements have the same order in any group.

To help us prove this result, we will first prove a lemma. In the next exercise you are asked to confirm some particular cases of this lemma, and then the lemma is stated with a general proof.

Exercise E74

Let x , y and g be elements of a group, and suppose that $y = gxg^{-1}$. Prove each of the following.

$$(a) \ y^2 = gx^2g^{-1} \quad (b) \ y^3 = gx^3g^{-1} \quad (c) \ y^4 = gx^4g^{-1}$$

From the solution to Exercise E74 it is apparent that the pattern in the exercise will continue for all positive integers n . In other words, the lemma below holds. To prove this result formally, we use mathematical induction, which you met in Unit A3 *Mathematical language and proof*.



Lemma E20

Let x , y and g be elements of a group, and suppose that $y = gxg^{-1}$. Then $y^n = gx^ng^{-1}$ for all positive integers n .

Proof We use mathematical induction. Let $P(n)$ be the statement

$$y^n = gx^ng^{-1}.$$

Then $P(1)$ is $y = gxg^{-1}$, which is true.

 We now need to show that $P(k) \implies P(k+1)$ for each positive integer k . 

Now let k be a positive integer and assume that $P(k)$ is true; that is,

$$y^k = gx^kg^{-1}.$$

We need to prove under this assumption that $P(k+1)$ is true, that is,


$$y^{k+1} = gx^{k+1}g^{-1}.$$

Now

$$\begin{aligned} y^{k+1} &= y^k y \\ &= gx^kg^{-1}gxg^{-1} \quad (\text{by } P(k) \text{ and since } y = gxg^{-1}) \\ &= gx^kexg^{-1} \\ &= gx^{k+1}g^{-1}. \end{aligned}$$

Thus $P(k+1)$ is true. So we have shown that

$$P(k) \implies P(k+1) \quad \text{for each positive integer } k.$$

Hence, by mathematical induction, it follows that $P(n)$ is true for all positive integers n . That is, $y^n = gx^ng^{-1}$ for all positive integers n . 

We can now prove the result below. Remember that the order of a group element x is the *smallest* positive integer n such that $x^n = e$, if there is such an integer n . If there is no such integer n , then x has infinite order.

Theorem E21

Let x and y be conjugate elements in a group G . Then either x and y have the same finite order, or they both have infinite order.

Proof Since x and y are conjugate elements, there exists an element g in G such that $y = gxg^{-1}$. It follows that $x = g^{-1}yg$.

We now show that for any positive integer n ,

$$x^n = e \quad \text{if and only if} \quad y^n = e. \quad (5)$$

To do this, let n be a positive integer, and first suppose that $x^n = e$. Then

$$\begin{aligned} y^n &= gx^n g^{-1} \quad (\text{by Lemma E20, since } y = gxg^{-1}) \\ &= geg^{-1} \\ &= e. \end{aligned}$$

Now suppose instead that $y^n = e$. Then

$$\begin{aligned} x^n &= g^{-1}y^n g \quad (\text{by Lemma E20, since } x = g^{-1}yg; \\ &\quad \text{here } g^{-1} \text{ is the conjugating element}) \\ &= g^{-1}eg \\ &= e. \end{aligned}$$

We have now shown that statement (5) holds. This statement tells us that the positive integers n for which $x^n = e$ are exactly the same as the positive integers n for which $y^n = e$. It follows that either x and y have the same finite order, or both have infinite order. ■

The converse of Theorem E21 is not true: that is, group elements of the same order are not necessarily conjugate. For example, in the symmetric group S_4 the permutations $(1\ 2)$ and $(1\ 2)(3\ 4)$ both have order 2, but they are not conjugate because they have different cycle structures.

Exercise E75

Find two elements in the group \mathbb{Z}_6 that have the same order but are not conjugate in \mathbb{Z}_6 .

2.3
Conjugacy classes

We now consider the set of all elements in a group that are conjugate to a particular element. We make the following definition.

Definition

Let G be a group, and let $x \in G$. The **conjugacy class** of x in G is the set of all elements of G that are conjugate to x . That is, it is the set

$$\{gxg^{-1} : g \in G\}.$$

Worked Exercise E27

Find the conjugacy class of the element a in $S(\square)$.
(The group table of $S(\square)$ is given as Table 6.)

Table 6 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

Solution

We find all the conjugates of a in $S(\square)$.

The conjugates of a in $S(\square)$ are

$$\begin{aligned}
 e \circ a \circ e^{-1} &= e \circ (a \circ e) = e \circ a = a, \\
 a \circ a \circ a^{-1} &= a \circ e = a, \\
 b \circ a \circ b^{-1} &= b \circ (a \circ b) = b \circ c = a, \\
 c \circ a \circ c^{-1} &= c \circ (a \circ a) = c \circ b = a, \\
 r \circ a \circ r^{-1} &= r \circ (a \circ r) = r \circ s = c, \\
 s \circ a \circ s^{-1} &= s \circ (a \circ s) = s \circ t = c, \\
 t \circ a \circ t^{-1} &= t \circ (a \circ t) = t \circ u = c, \\
 u \circ a \circ u^{-1} &= u \circ (a \circ u) = u \circ r = c.
 \end{aligned}$$

There are only two distinct conjugates: a and c .

So the conjugacy class of a in $S(\square)$ is $\{a, c\}$.

Exercise E76

Find the conjugacy class of each of the following elements in $S(\square)$.
(a) c (b) e

A group element is always an element of its own conjugacy class, as illustrated by the solutions to Worked Exercise E27 and Exercise E76. This is because conjugating a group element x by the identity element e always gives x again: $exe^{-1} = x$.

If we extend the calculations in Worked Exercise E27 and Exercise E76 to find the conjugacy class of every element of $S(\square)$, then we obtain the following.

| Element | Conjugacy class |
|---------|-----------------|
| e | $\{e\}$ |
| a | $\{a, c\}$ |
| b | $\{b\}$ |
| c | $\{a, c\}$ |
| r | $\{r, t\}$ |
| s | $\{s, u\}$ |
| t | $\{r, t\}$ |
| u | $\{s, u\}$ |

Notice that some of the conjugacy classes here are the same; in fact, there are only five *distinct* conjugacy classes, as follows:

$$\{e\}, \quad \{b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

Notice also that there is no overlap between any two of the distinct conjugacy classes: the conjugacy classes of any two elements in $S(\square)$ are either exactly the same set or disjoint sets. Thus the distinct conjugacy classes of the elements of $S(\square)$ form a *partition* of $S(\square)$, as shown in Figure 13. That is, they split $S(\square)$ into a family of subsets whose union is the whole group, and each pair of which are disjoint.

In fact, like the left (or right) cosets of a subgroup, the distinct conjugacy classes of the elements of any group form a partition of the group.

This is because, as proved below, the relation ‘is a conjugate of’, defined on any group, is an *equivalence relation*, and the conjugacy classes are its equivalence classes. (You met equivalence relations in Unit A3.) In fact, you have already seen that the relation ‘is a conjugate of’ on any group has the *reflexive property*: you saw that each element x is a conjugate of itself. You have also seen that it has the *symmetric property*: you saw that if y is a conjugate of x , then x is a conjugate of y . The third property that has to be satisfied for a relation to be an equivalence relation is the *transitive property*. The proof below reminds you of its definition, and includes proofs of all three properties, for completeness.

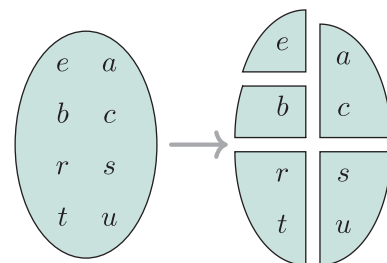


Figure 13 The partition of $S(\square)$ into conjugacy classes

Theorem E22

Let G be a group. Then the relation ‘is a conjugate of’ is an equivalence relation on the set of elements of G .



Proof We show that the relation ‘is a conjugate of’ defined on G is reflexive, symmetric and transitive.

E1 Reflexive property

 We have to show that for all $x \in G$, x is a conjugate of x . 

Let $x \in G$. Then $x = exe^{-1}$, so x is a conjugate of x . Thus the relation is reflexive.

E2 Symmetric property

 We have to show that for all $x, y \in G$, if x is a conjugate of y then y is a conjugate of x . 

Let $x, y \in G$, and suppose that x is a conjugate of y . Then there is an element $g \in G$ such that

$$x = gyg^{-1}.$$

Composing both sides of this equation on the left by g^{-1} and on the right by g , we obtain



$$g^{-1}xg = y,$$

and this equation can be written as

$$y = g^{-1}x(g^{-1})^{-1}.$$

Thus g^{-1} conjugates x to y , so y is a conjugate of x . Thus the relation is symmetric.

E3 Transitive property

 We have to show that for all $x, y, z \in G$, if x is a conjugate of y and y is a conjugate of z then x is a conjugate of z . 

Let $x, y, z \in G$, and suppose that x is a conjugate of y and y is a conjugate of z . Then there are elements g_1 and g_2 in G such that

$$x = g_1yg_1^{-1} \quad \text{and} \quad y = g_2zg_2^{-1}.$$

Using the second equation to substitute for y in the first equation gives

$$x = g_1g_2zg_2^{-1}g_1^{-1},$$

which (by Proposition B14 in Unit B1) we can write as

$$x = g_1g_2z(g_1g_2)^{-1}.$$

Thus g_1g_2 conjugates z to x , so x is a conjugate of z . Thus the relation is transitive.

Hence the relation ‘is a conjugate of’ is an equivalence relation on G . 

From Theorem E22 we can deduce the following, illustrated in Figure 14.

Corollary E23

In any group, the distinct conjugacy classes form a partition of the group.

Proof The conjugacy class of an element x of a group G is the set of all elements of G that are conjugate to x . In other words, it is the equivalence class of x with respect to the equivalence relation ‘is a conjugate of’ defined on G . So the distinct conjugacy classes are the distinct equivalence classes of this equivalence relation, and hence they partition G . ■

We refer to the distinct conjugacy classes of the elements of a group G as the **conjugacy classes of G** . For example, you saw after Exercise E76 that the conjugacy classes of $S(\square)$ are

$$\{e\}, \quad \{b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

Every group has at least one conjugacy class that is quick to find. As you saw in Exercise E73(a), conjugating the identity element e of a group by any other element g just gives the identity element again: $geg^{-1} = gg^{-1} = e$. So the following holds.

Proposition E24

Let G be a group with identity element e . Then $\{e\}$ is a conjugacy class of G .

For a *finite* group G , we can find all the other conjugacy classes of G by working out the conjugacy class of each element, in the way demonstrated in Worked Exercise E27 and Exercise E76, and then assembling all the distinct conjugacy classes.

A much more efficient method, which applies because the conjugacy classes partition the group, is to use a strategy similar to the one that we used for cosets of a subgroup: we repeatedly choose an element not yet assigned to a conjugacy class and find its conjugacy class, until all the elements have been assigned to conjugacy classes.

However, there are usually still more efficient ways to proceed. For example, we can sometimes cut down the work by using the fact that conjugate elements always have the same order, by Theorem E21.

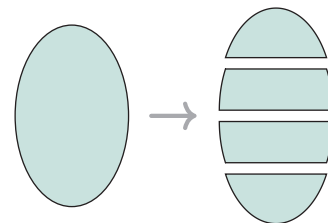


Figure 14 The partition of a group into conjugacy classes

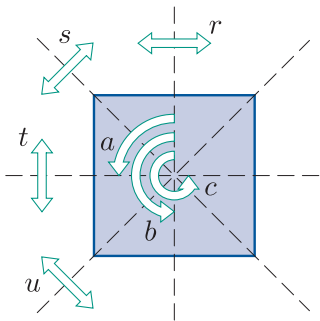


Figure 15 $S(\square)$

To illustrate this, let us use this approach to confirm that the conjugacy classes of $S(\square)$ are as listed above. The non-identity elements of $S(\square)$ are shown in Figure 15. We know that elements of different orders cannot be conjugate, so to partition $S(\square)$ into conjugacy classes we can start by partitioning it according to the orders of its elements. The identity element has order 1, the elements a and c both have order 4, and the elements b, r, s, t and u all have order 2, so the partition of $S(\square)$ by the orders of its elements is

$$\{e\}, \quad \{a, c\}, \quad \{b, r, s, t, u\}.$$

We know that each conjugacy class of $S(\square)$ is either one of these three sets or is obtained by splitting one of these sets into two or more conjugacy classes.

To determine whether the set $\{a, c\}$, for example, is a conjugacy class or whether it splits further, we can start conjugating the element a by each element of $S(\square)$ in turn. If we find a conjugate that is equal to c , then this tells us that $\{a, c\}$ is a conjugacy class, and there is no need to find any more conjugates. On the other hand, if after conjugating a by all the elements of $S(\square)$ we have found that no conjugate of a is equal to c , then this tells us that the set $\{a, c\}$ must split into the two conjugacy classes $\{a\}$ and $\{c\}$. We can carry out a similar process for the set $\{b, r, s, t, u\}$.

This method is demonstrated in the worked exercise below.

Worked Exercise E28

Find the conjugacy classes of the group $S(\square)$.

(The group table of $S(\square)$ is given as Table 7.)

Table 7 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

Solution

Start by partitioning $S(\square)$ by the orders of its elements.

The partition of $S(\square)$ by the orders of its elements is

$$\{e\}, \quad \{a, c\}, \quad \{b, r, s, t, u\}.$$

Hence the set $\{e\}$ is a conjugacy class.

Consider the set $\{a, c\}$.

We find conjugates of a to see if we can obtain c . There is no point in conjugating a by any of the elements e, a, b or c , as that will give a again, since $\{e, a, b, c\}$ is an abelian subgroup of $S(\square)$. Let us try conjugating a by r .

We have

$$r \circ a \circ r^{-1} = r \circ (a \circ r) = r \circ s = c.$$

Hence $\{a, c\}$ is a conjugacy class.

Now consider the set $\{b, r, s, t, u\}$.

☁ We find conjugates of b to see if we can obtain any of r, s, t and u . ☁

Conjugating b by any of e, a, b or c will give b again, since $\{e, a, b, c\}$ is an abelian subgroup of $S(\square)$. Also,

$$\begin{aligned} r \circ b \circ r^{-1} &= r \circ (b \circ r) = r \circ t = b, \\ s \circ b \circ s^{-1} &= s \circ (b \circ s) = s \circ u = b, \\ t \circ b \circ t^{-1} &= t \circ (b \circ t) = t \circ r = b, \\ u \circ b \circ u^{-1} &= u \circ (b \circ u) = u \circ s = b. \end{aligned}$$

Hence $\{b\}$ is a conjugacy class.

☁ Now we find conjugates of r to see if we can obtain any of s, t and u . ☁

Conjugating r by e or r will give r . Also,

$$\begin{aligned} a \circ r \circ a^{-1} &= a \circ (r \circ c) = a \circ s = t, \\ b \circ r \circ b^{-1} &= b \circ (r \circ b) = b \circ t = r, \\ c \circ r \circ c^{-1} &= c \circ (r \circ a) = c \circ u = t, \\ s \circ r \circ s^{-1} &= s \circ (r \circ s) = s \circ c = t, \\ t \circ r \circ t^{-1} &= t \circ (r \circ t) = t \circ b = r, \\ u \circ r \circ u^{-1} &= u \circ (r \circ u) = u \circ a = t. \end{aligned}$$

Hence $\{r, t\}$ is a conjugacy class.

☁ Now we just need to find conjugates of s to see if we can obtain u . We know that conjugating s by e or s will give s again. Let us try conjugating s by a . ☁

Finally, we have

$$a \circ s \circ a^{-1} = a \circ (s \circ c) = a \circ t = u.$$

Hence $\{s, u\}$ is a conjugacy class.

In summary, the conjugacy classes of $S(\square)$ are

$$\{e\}, \quad \{a, c\}, \quad \{b\}, \quad \{r, t\}, \quad \{s, u\}.$$

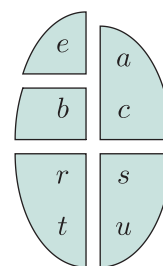


Figure 16 The conjugacy classes of $S(\square)$

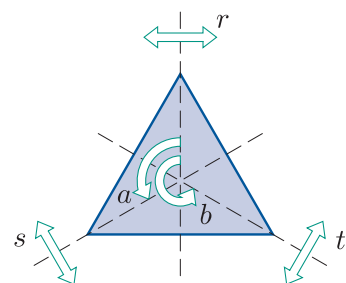


Figure 17 The symmetries of the equilateral triangle

The partition of $S(\square)$ into conjugacy classes is shown in Figure 16.

Exercise E77

Find the conjugacy classes of the group $S(\triangle)$.

(The non-identity elements of $S(\triangle)$ are shown in Figure 17, and the group table of $S(\triangle)$ is given as Table 8.)

Table 8 $S(\triangle)$

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

For *symmetry groups*, such as $S(\square)$ and $S(\triangle)$, there are in fact very efficient ways to find the conjugacy classes, as you will see in Section 4.

Exercise E78

Partition the group \mathbb{Z}_7^* into its conjugacy classes.

Hint: Use the result proved in Exercise E72 in Subsection 2.2.

Exercise E78 illustrates the following result (it is just the result proved in the solution to Exercise E72 restated in terms of conjugacy classes).

Theorem E25

In an abelian group, each conjugacy class contains a single element.

Proof Let G be an abelian group and let x be any element of G . Since G is abelian, for any element $g \in G$ we have

$$gxg^{-1} = gg^{-1}x = ex = x.$$

So the only conjugate of x is x itself. Hence the conjugacy class of x is $\{x\}$. ■

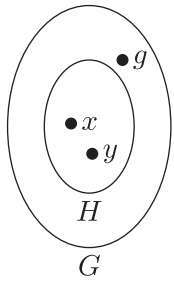


Figure 18 Elements x , y and g in a group G with a subgroup H

Whenever you work with conjugates, you need to be aware of the following important but quite subtle point. When we say that *elements x and y are conjugate in the group G* , the ‘in the group G ’ part is crucial. This is because if H is a subgroup of a group G and x and y are elements of H , as illustrated in Figure 18, then it is possible for x and y to be conjugate in G but not conjugate in H . The reason for this is that if x and y are conjugate in G , then although we know that there is an element g in G such that $y = gxg^{-1}$, as also illustrated in Figure 18, there may not be any such element g in the subgroup H .

For example, consider the group $S(\square)$. As you saw in Subsection 2.4 of Unit B3, we can represent this group as a subgroup of the symmetric group S_4 by representing its elements as permutations of vertex labels (see Figure 19), as follows.

$$\begin{array}{ll} e & r = (1\ 4)(2\ 3) \\ a = (1\ 2\ 3\ 4) & s = (2\ 4) \\ b = (1\ 3)(2\ 4) & t = (1\ 2)(3\ 4) \\ c = (1\ 4\ 3\ 2) & u = (1\ 3) \end{array}$$

The conjugacy classes of $S(\square)$, found in Worked Exercise E28, are

$$\{e\}, \quad \{b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

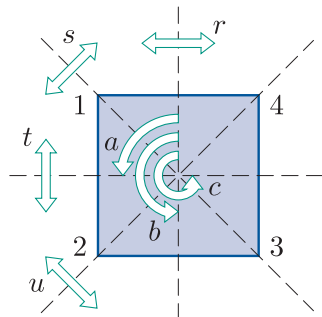


Figure 19 $S(\square)$

With the elements of $S(\square)$ represented as permutations as above, these conjugacy classes are

$$\{e\}, \quad \{(1\ 3)(2\ 4)\}, \quad \{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}, \\ \{(1\ 4)(2\ 3), (1\ 2)(3\ 4)\}, \quad \{(2\ 4), (1\ 3)\}.$$

So the elements $b = (1\ 3)(2\ 4)$ and $r = (1\ 4)(2\ 3)$, for example, are *not* conjugate in $S(\square)$. However, they *are* conjugate in the group S_4 because they have the same cycle structure. So although there is an element g in S_4 that conjugates $b = (1\ 3)(2\ 4)$ to $r = (1\ 4)(2\ 3)$, there is no such element g in the subgroup $S(\square)$ of S_4 .

Now consider again the general situation where a group H is a subgroup of a group G and x and y are elements of H , as illustrated in Figure 18 above. You have seen that if x and y are conjugate in G , then they are not necessarily conjugate in H . However, if x and y are conjugate in H , then they are also conjugate in G . This is because if x and y are conjugate in H , then there is an element h of H such that $y = h x h^{-1}$, as illustrated in Figure 20, and since $h \in G$ this equation shows that x and y are conjugate in G .

The discussion above proves the following proposition.

Proposition E26

Let H be a subgroup of a group G , and let x and y be elements of H .

- (a) If x and y are conjugate in H , then they are also conjugate in G .
- (b) If x and y are conjugate in G , then they may or may not be conjugate in H .

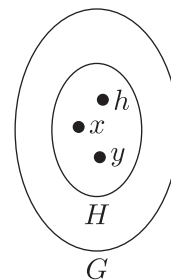


Figure 20 Elements x , y and h in a subgroup H of a group G

The contrapositive of Proposition E26(a) is:

If x and y are not conjugate in G , then they are not conjugate in H .

This fact will be useful later in the unit.

Exercise E79

Consider the subgroup

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

of the group S_4 (this subgroup represents the symmetry group of the rectangle when its vertices are labelled in the usual way, as shown in Figure 21). Explain how you know that no two elements of H are conjugate to each other in H , but all the non-identity elements of H are conjugate to each other in S_4 .

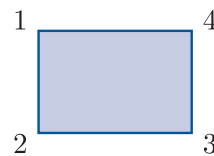


Figure 21 A labelled rectangle

Notice that the representation of the elements of $S(\square)$ as permutations,

$$\begin{array}{ll} e, & r = (1\ 4)(2\ 3), \\ a = (1\ 2\ 3\ 4), & s = (2\ 4), \\ b = (1\ 3)(2\ 4), & t = (1\ 2)(3\ 4), \\ c = (1\ 4\ 3\ 2), & u = (1\ 3), \end{array}$$

makes it clear that the elements r and t of $S(\square)$ do not lie in the same conjugacy class of $S(\square)$ as the elements s and u , as follows. The cycle structure $(- -)(- -)$ of r and t is different from the cycle structure $(- -)$ of s and u , so neither of r and t is conjugate to either of s and u in S_4 , and hence the same must be true in the subgroup $S(\square)$ of S_4 . We will use this idea, and others, to help us find conjugacy classes of symmetry groups in Section 4.

We end this subsection with a useful result about the conjugacy classes of finite groups.

To illustrate it, consider the conjugacy classes of the group $S(\square)$. You have seen that they are as follows:

$$\{e\}, \quad \{b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

The numbers of elements in these conjugacy classes are 1, 1, 2, 2 and 2, respectively, and each of these numbers divides 8, the order of $S(\square)$.

A similar fact is true for the conjugacy classes of the group $S(\triangle)$, which as you have seen are as follows:

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

The numbers of elements in these conjugacy classes are 1, 2 and 3, respectively, and each of these numbers divides 6, the order of $S(\triangle)$.

The following general result holds. It is proved in Unit E4.

Theorem E27

In any finite group G , the number of elements in each conjugacy class divides the order of G .

3 Normal subgroups and conjugacy

In Unit E1 you saw that a subgroup H of a group G is a **normal subgroup** of G if the partition of G into left cosets of H is the same as the partition of G into right cosets of H . You saw that this condition can be expressed algebraically as

$$gH = Hg \quad \text{for each element } g \in G.$$

In this section you will meet three conditions that are equivalent to this condition, and that we can therefore use as alternatives to check whether

a subgroup is normal. These three conditions all involve conjugacy, and are often more convenient than the condition above.

We refer to checking whether a subgroup is normal or not as checking its **normality**.

3.1 Normal subgroups and conjugates

In this first subsection you will meet a condition for normality that involves conjugate elements.

To introduce it, let us suppose that we know that a particular subgroup H of a group G is a normal subgroup of G . Let h and g be any elements of H and G , respectively. Then, by the definition of a left coset,

$$gh \in gH.$$

Hence, since H is normal and so $gH = Hg$,

$$gh \in Hg.$$

Therefore

$$gh = h_1g$$

for some element $h_1 \in H$. Composing both sides of this equation on the right by g^{-1} gives

$$ghg^{-1} = h_1.$$

Hence

$$ghg^{-1} \in H.$$

So we have found that, as illustrated in Figure 22,

if H is a normal subgroup of a group G , then for any element h in H and any element g in G , the conjugate ghg^{-1} always lies in H .

In other words,

if H is a normal subgroup of a group G , then conjugating any element of H by any element of G always gives an element of H .

It turns out that the converse of this statement is also true; that is,

if conjugating any element of a subgroup H of a group G by any element of G always gives an element of H , then H is normal in G .

Hence we have the following theorem. It is proved fully in Subsection 3.4.

Theorem E28

Let G be a group and let H be a subgroup of G . Then H is a normal subgroup of G if and only if

$$ghg^{-1} \in H \quad \text{for each } h \in H \text{ and each } g \in G.$$

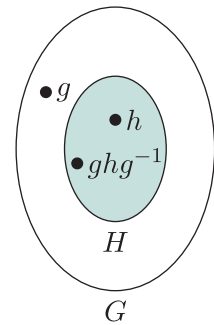


Figure 22 A normal subgroup H of a group G : conjugating any element of H by any element of G always gives an element of H

Theorem E28 gives us an alternative way to determine whether a subgroup is normal: we say that it **characterises** normal subgroups.

The characterisation of normal subgroups in Theorem E28 is more useful than our original definition of a normal subgroup for groups of large order or infinite order. To use it to prove that a subgroup H of a group G is normal in G , we take a general element $g \in G$ and a general element $h \in H$, and show that the conjugate ghg^{-1} belongs to H . As an illustration of this, here are alternative proofs of two results that you met in Unit E1.

Theorem E10

In an abelian group, every subgroup is normal.

Proof Let H be a subgroup of an abelian group G . We use Theorem E28 to show that H is normal in G . Let h be any element of H and let g be any element of G . We need to show that $ghg^{-1} \in H$.

We have

$$\begin{aligned} ghg^{-1} &= hgg^{-1} \quad (\text{since } G \text{ is abelian}) \\ &= he \\ &= h. \end{aligned}$$

Thus $ghg^{-1} \in H$. It follows that H is a normal subgroup of G . ■

Corollary E12

For each natural number n , the alternating group A_n is a normal subgroup of the symmetric group S_n .

Proof We use Theorem E28 to show that A_n is normal in S_n . Let h be any element of A_n and let g be any element of S_n . We have to show that $g \circ h \circ g^{-1} \in A_n$, that is, we have to show that $g \circ h \circ g^{-1}$ is an even permutation. We consider separately the possibilities that g is even and that g is odd.

If g is even, then g^{-1} is even and hence $g \circ h \circ g^{-1}$ is

$$\text{even} + \text{even} + \text{even} = \text{even}.$$

If g is odd, then g^{-1} is odd and hence $g \circ h \circ g^{-1}$ is

$$\text{odd} + \text{even} + \text{odd} = \text{even}.$$

Thus, in each case, $g \circ h \circ g^{-1} \in A_n$. It follows that A_n is a normal subgroup of S_n . ■

Here are some exercises in which you can practise using Theorem E28.

Exercise E80

Use Theorem E28 to provide an alternative proof of Theorem E9 in Unit E1. That is, prove that for any group G the trivial subgroup $\{e\}$ and the whole group G are normal subgroups of G .

Exercise E81

By Theorem B81 in Unit B4 *Lagrange's Theorem and small groups*, if H and K are subgroups of a group G , then so is $H \cap K$. Use this result and Theorem E28 to prove that if H and K are normal subgroups of a group G , then so is $H \cap K$.

Exercise E82

In Worked Exercise B18 in Subsection 1.2 of Unit B2 you met the group $(X, *)$ where X is the subset of \mathbb{R}^2 consisting of all the points not on the y -axis, that is,

$$X = \{(a, b) \in \mathbb{R}^2 : a \neq 0\},$$

and $*$ is the binary operation defined on X by

$$(a, b) * (c, d) = (ac, ad + b).$$

It was shown that in this group the identity element is $(1, 0)$ and the inverse of the element (a, b) is $\left(\frac{1}{a}, -\frac{b}{a}\right)$.

(a) As a reminder, verify the following in $(X, *)$.

- (i) $(a, b) * (1, 0) = (a, b)$ for all $(a, b) \in X$.
- (ii) $\left(\frac{1}{a}, -\frac{b}{a}\right) * (a, b) = (1, 0)$ for all $(a, b) \in X$.

(b) Determine the following conjugates in $(X, *)$

- (i) $(3, 2) * (1, 7) * (3, 2)^{-1}$
- (ii) $(-1, 3) * (1, -2) * (-1, 3)^{-1}$

(c) In the same worked exercise, Worked Exercise B18, you also saw that the set

$$A = \{(1, b) : b \in \mathbb{R}\}$$

is a subgroup of the group $(X, *)$.

Use Theorem E28 to prove that this subgroup A is normal in $(X, *)$.

Hint: Remember that a general element of X is of the form (c, d) , say, where $c, d \in \mathbb{R}$ and $c \neq 0$, and a general element of A is of the form $(1, b)$, say, where $b \in \mathbb{R}$.

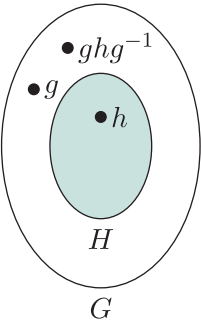


Figure 23 A subgroup H that is not normal in a group G : there is an element h of H and an element g of G such that conjugating h by g does not give an element of H

Table 9 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

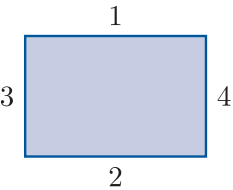


Figure 24 A rectangle with labelled edges

The characterisation of normal subgroups in Theorem E28 also provides a useful means of showing that a subgroup H of a group G is *not* normal in G . To do this, we have to show that H and G do not satisfy the condition in the theorem, by giving a counterexample. That is, we have to find *one* element h in H and *one* element g in G such that the conjugate ghg^{-1} does not belong to H , as illustrated in Figure 23.

Worked Exercise E29

Use Theorem E28 to show that the subgroup

$$H = \langle r \rangle = \{e, r\}$$

of $S(\square)$ is not a normal subgroup of $S(\square)$.

(The group table of $S(\square)$ is given as Table 9.)

Solution

By experimentation, we find an element $g \in S(\square)$ and an element $h \in H$ such that the conjugate $g \circ h \circ g^{-1}$ does not belong to H . We can ignore e as a possibility for the element of H , since $g \circ e \circ g^{-1} = e$ for all $g \in S(\square)$, so the only possibility for the element of H is r .

We have $r \in H$ and $a \in S(\square)$, but

$$a \circ r \circ a^{-1} = t \notin H.$$

Therefore by Theorem E28 the subgroup H is not normal in G .

Exercise E83

Use Theorem E28 to prove that the following subgroups of S_4 are not normal subgroups of S_4 .

- (a) $H = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$, the symmetry group of the rectangle when its edges are labelled as shown in Figure 24.
- (b) $H = \{g \in S_4 : g(2) = 2\}$, the subgroup of all permutations in S_4 that fix the symbol 2.

Exercise E84

Let $(X, *)$ be the group defined in Exercise E82.

Show that the subset

$$K = \{(1, n) : n \in \mathbb{Z}\}$$

of X is a subgroup of X , and determine whether it is a normal subgroup of X .

3.2 Conjugate subgroups

In this subsection you will see that the idea of *conjugate subgroups*, which you met in the context of symmetric groups in Unit B3, can be extended to other groups. This leads to another characterisation of normal subgroups.

In Subsection 4.2 of Unit B3 you met the idea of conjugating a whole subgroup H of a symmetric group S_n by a permutation g in S_n , as follows.

Notation

Let H be a subgroup of S_n , and let g be any permutation in S_n . Then

$$g \circ H \circ g^{-1} \text{ denotes the set } \{g \circ h \circ g^{-1} : h \in H\}.$$

That is, $g \circ H \circ g^{-1}$ is the set obtained by conjugating every element of H by the permutation g .

You saw that if H is a subgroup of S_n , then for every permutation g in S_n the set $g \circ H \circ g^{-1}$ is also a subgroup of S_n : this is Theorem B65 in Unit B3. We say that the subgroup $g \circ H \circ g^{-1}$ is a **conjugate subgroup** of H in S_n .

We can extend these ideas to groups in general. We use the following notation.

Notation

Let H be a subgroup of a group G , and let g be any element of G . Then

$$gHg^{-1} \text{ denotes the set } \{ghg^{-1} : h \in H\}.$$

That is, gHg^{-1} is the set obtained by conjugating every element of H by the element g .

The theorem below generalises Theorem B65 from symmetric groups to all groups.

Theorem E29

Let H be a subgroup of a group G and let g be any element of G . Then the subset gHg^{-1} is a subgroup of G .

Proof We check the three subgroup properties.

SG1 Closure Consider any two elements of gHg^{-1} ; we can write them as ghg^{-1} and gkg^{-1} where $h, k \in H$. We have

$$\begin{aligned}(ghg^{-1})(gkg^{-1}) &= gh(g^{-1}g)kg^{-1} \\ &= ghekg^{-1} \\ &= ghkg^{-1}.\end{aligned}$$

This is an element of gHg^{-1} because hk is an element of H (since H is a subgroup of G and therefore closed under the binary operation of G). Thus gHg^{-1} is closed under the binary operation of G .

SG2 Identity The identity permutation e is in gHg^{-1} since $e = geg^{-1}$ and $e \in H$.

SG3 Inverses Consider any element of gHg^{-1} ; we can write it as ghg^{-1} where $h \in H$. We have

$$\begin{aligned}(ghg^{-1})^{-1} &= (g^{-1})^{-1}h^{-1}g^{-1} \\ &\quad \text{(by Proposition B14 in Unit B1, applied twice)} \\ &= gh^{-1}g^{-1}.\end{aligned}$$

This is an element of gHg^{-1} because h^{-1} is an element of H (since H is a subgroup of G and therefore contains the inverse of each of its elements). Thus gHg^{-1} contains the inverse of each of its elements.

Since gHg^{-1} satisfies the three subgroup properties, it is a subgroup of G . ■

We can now make the following definitions.

Definitions

Let H be a subgroup of a group G and let g be an element of G . We call the subgroup gHg^{-1} the **conjugate subgroup** of H by g . We also say that

- gHg^{-1} is a **conjugate subgroup** of H in G
- g **conjugates** H to gHg^{-1} .

Although we used notation of the form $g \circ H \circ g^{-1}$ for conjugate subgroups (in symmetric groups) in Unit B3, in Book E we will use notation of the form gHg^{-1} , for brevity, even if we are using the symbol \circ to denote the binary operation.

Worked Exercise E30

Let H be the subgroup $\langle t \rangle = \{e, t\}$ of $S(\triangle)$. Determine the conjugate subgroup aHa^{-1} .

(The non-identity elements of $S(\triangle)$ are shown in Figure 25, and the group table of $S(\triangle)$ is given as Table 10.)

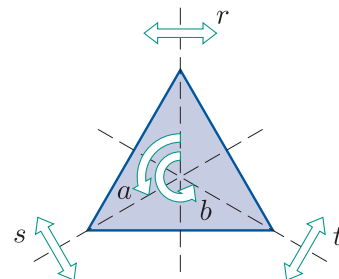


Figure 25 The symmetries of the equilateral triangle

Solution

We have

$$aHa^{-1} = \{a \circ e \circ a^{-1}, a \circ t \circ a^{-1}\}.$$

Now

$$a \circ e \circ a^{-1} = a \circ a^{-1} = e,$$

$$a \circ t \circ a^{-1} = (a \circ t) \circ b = s \circ b = r.$$

So

$$aHa^{-1} = \{e, r\}.$$

Table 10 $S(\triangle)$

| \circ | e | a | b | r | s | t |
|---------|-----|-----|-----|-----|-----|-----|
| e | e | a | b | r | s | t |
| a | a | b | e | t | r | s |
| b | b | e | a | s | t | r |
| r | r | s | t | e | a | b |
| s | s | t | r | b | e | a |
| t | t | r | s | a | b | e |

Exercise E85

Determine the conjugate subgroup gHg^{-1} in the group $S(\square)$ in each of the following cases.

- (a) $H = \langle s \rangle = \{e, s\}$ and $g = a$ (b) $H = \{e, b, s, u\}$ and $g = r$

(The group table of $S(\square)$ is given as Table 11. You saw that the set H in part (b) is a subgroup of $S(\square)$ in Exercise E15 in Subsection 1.4 of Unit E1.)

Table 11 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

In Subsection 2.2 you saw that if x and y are elements of a group G and the element g of G conjugates x to y , then g^{-1} conjugates y to x . It follows that if H and K are subgroups of a group G , and the element g of G conjugates H to K , then g^{-1} conjugates K to H . Because of this, instead of saying that K is a conjugate subgroup of H in G , we can simply say that H and K are **conjugate subgroups** in G .

Conjugate subgroups have the following property.

Proposition E30

Let H and K be conjugate subgroups in a group G . Then either H and K have the same finite order, or they both have infinite order.

Proof Since H and K are conjugate subgroups in G , there is an element g of G such that $K = gHg^{-1}$. Consider the following mapping:

$$\begin{aligned}\phi : H &\longrightarrow K \\ x &\longmapsto gxg^{-1}.\end{aligned}$$

This mapping ϕ is onto, since every element of K is of the form gxg^{-1} where $x \in H$. Also, it is one-to-one, since if $x, y \in H$ and $gxg^{-1} = gyg^{-1}$ then $x = y$, by the Cancellation Laws.

Thus ϕ is a one-to-one correspondence, which proves the required result. ■



Figure 26 A labelled rectangle

Exercise E86

Consider the following subgroup K of A_4 :

$$K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

(It is the symmetry group of the rectangle when its vertices are labelled in the usual way, as shown in Figure 26.)

- (a) By conjugating each element of K individually, determine the following conjugate subgroups of K in A_4 .

$$(i) \ (1\ 2\ 4)K(1\ 2\ 4)^{-1} \quad (ii) \ (2\ 4\ 3)K(2\ 4\ 3)^{-1}$$

- (b) Without calculating any further conjugates, determine how many different conjugate subgroups K has in A_4 .

Hint: Remember that conjugating a permutation does not change its cycle structure.

You saw in Exercise E86(b) that the subgroup

$$K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

of the group A_4 has the property that

$$gKg^{-1} = K \quad \text{for each element } g \in A_4.$$

In other words, conjugating K by any element of A_4 just gives K again. You also saw in Exercise E47 in Section 5 of Unit E1 that this same subgroup K is a normal subgroup of A_4 .

These two properties of this subgroup K are linked: it turns out that if a subgroup H of a group G has the property that conjugating H by any element of G always gives H again, then H is normal in G , and that the converse of this result also holds. That is, we have the theorem below. This theorem provides our second alternative characterisation of normality. It is proved in Subsection 3.4.

Theorem E31

Let G be a group and let H be a subgroup of G . Then H is a normal subgroup of G if and only if

$$gHg^{-1} = H \quad \text{for each } g \in G.$$

You may be wondering whether Theorem E31 is really just another way of expressing Theorem E28, our previous characterisation of normality. However, Theorem E28 can be expressed as follows, which shows that Theorem E31 is not quite the same.

Theorem E28 (expressed differently)

Let G be a group and let H be a subgroup of G . Then H is a normal subgroup of G if and only if

$$gHg^{-1} \subseteq H \quad \text{for each } g \in G.$$

The characterisation of normality in Theorem E31 is interesting, but it turns out to be less useful in practice than the other two new characterisations given in this section.

3.3 Normal subgroups and conjugacy classes

This subsection gives the third of our three alternative characterisations of normality. It is closely related to the characterisation given in the previous subsection, but more useful in practice.

Recall that the *conjugacy class* of an element x in a group G is the subset of G consisting of all the elements of G that are conjugate to x :

$$\{gxg^{-1} : g \in G\}.$$

It can contain just the element x itself, or it can contain x together with further elements. The distinct conjugacy classes of the elements of a group G partition G , and we refer to them as the conjugacy classes of G .

Now suppose that H is a normal subgroup of a group G . We know from Theorem E28 (our first alternative characterisation of normality) that if $h \in H$ then every conjugate of h in G belongs to H . In other words, if $h \in H$ then the entire conjugacy class of h in G is a subset of H .

So each conjugacy class of G is either wholly inside H or wholly outside H : it cannot lie partly inside and partly outside.

So the following statement holds:

A normal subgroup is a union of conjugacy classes.

(Here a ‘union of conjugacy classes’ includes the possibility of a trivial union of just one class.)

It turns out that the following statement is also true:

Any subgroup of G that is a union of conjugacy classes of G is a normal subgroup of G .

Together these two facts give the following third alternative characterisation of normal subgroups. It is illustrated in Figures 27 and 28. As with the earlier characterisations, it is proved in Subsection 3.4.

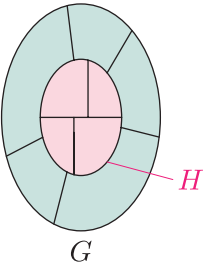


Figure 27 A normal subgroup H of a group G : each conjugacy class of G lies either entirely inside or entirely outside H

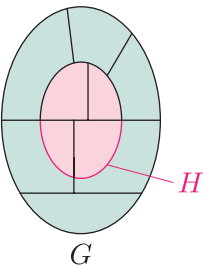


Figure 28 A subgroup H of a group G that is not normal: some conjugacy classes of G lie partly inside and partly outside H

Theorem E32

Let G be a group and let H be a subgroup of G . Then H is a normal subgroup of G if and only if

H is a union of conjugacy classes of G .

By Theorem E32, if we know the conjugacy classes of a group G , then we can use them to determine whether any subgroup of G is normal in G . In the remainder of this subsection we will look at several examples that illustrate this use of Theorem E32.

Worked Exercise E31

Given that the subgroups of $S(\square)$ are as follows, find all the normal subgroups of $S(\square)$.

| Order | Subgroup |
|-------|--|
| 1 | $\{e\}$ |
| 2 | $\{e, b\}, \{e, r\}, \{e, s\}, \{e, t\}, \{e, u\}$ |
| 4 | $\{e, a, b, c\}, \{e, b, r, t\}, \{e, b, s, u\}$ |
| 8 | $S(\square)$ |

Solution

In Worked Exercise E28 in Subsection 2.3 we found that the conjugacy classes of $S(\square)$ are

$\{e\}, \{a, c\}, \{b\}, \{r, t\}, \{s, u\}$.

Six of the ten subgroups of $S(\square)$ are unions of conjugacy classes, as follows.

$$\{e\} = \{e\}$$

$$\{e, b\} = \{e\} \cup \{b\}$$

$$\{e, a, b, c\} = \{e\} \cup \{a, c\} \cup \{b\}$$

$$\{e, b, r, t\} = \{e\} \cup \{b\} \cup \{r, t\}$$

$$\{e, b, s, u\} = \{e\} \cup \{b\} \cup \{s, u\}$$

$$S(\square) = \{e\} \cup \{a, c\} \cup \{b\} \cup \{r, t\} \cup \{s, u\}$$

Hence by Theorem E32 these six subgroups are normal subgroups of $S(\square)$.

The remaining four subgroups $\{e, r\}$, $\{e, s\}$, $\{e, t\}$ and $\{e, u\}$ of $S(\square)$ are not normal, since none of them can be expressed as a union of conjugacy classes.

Exercise E87

Given that the subgroups of the group $S(\triangle)$ are as follows, find all the normal subgroups of $S(\triangle)$.

| Order | Subgroup |
|-------|--------------------------------|
| 1 | $\{e\}$ |
| 2 | $\{e, a, b\}$ |
| 3 | $\{e, r\}, \{e, s\}, \{e, t\}$ |
| 6 | $S(\triangle)$ |

(The conjugacy classes of $S(\triangle)$ are

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

You were asked to find them in Exercise E77 in Subsection 2.3.)

In each of Worked Exercise E31 and Exercise E87 we found all the normal subgroups of a finite group by starting with all the subgroups and working out which of them are unions of conjugacy classes. However, often we do not know all the subgroups of a group or there may be a large number of them, so it can be better to instead start with the conjugacy classes and work out which unions of conjugacy classes are subgroups. We can immediately dismiss as possibilities any unions of conjugacy classes that do not contain the identity element. We can also immediately dismiss any unions of conjugacy classes whose total number of elements is not a divisor of the order of G , in view of Lagrange's Theorem. We then need to determine which of the remaining possibilities are subgroups.

This approach is illustrated in the next worked exercise, in which we find all the normal subgroups of the symmetric group S_4 . Remember that for a symmetric group the partition into conjugacy classes is the same as the partition by cycle structure (by Theorem B64, repeated in Subsection 2.1).



Worked Exercise E32

Given that the numbers of elements in the conjugacy classes of the symmetric group S_4 are as follows, determine all the normal subgroups of S_4 .

| Conjugacy class | Cycle structure | Number of elements |
|-----------------|-----------------|--------------------|
| A | e | 1 |
| B | $(- -)$ | 6 |
| C | $(- - -)$ | 8 |
| D | $(- - - -)$ | 6 |
| E | $(- -)(- -)$ | 3 |

(The numbers of elements of S_4 with cycle structures e , $(- - -)$ and $(- -)(- -)$ were worked out in Subsection 3.3 of Unit B3. The numbers of elements with cycle structures $(- -)$ and $(- - - -)$ can be worked out in similar ways.)

Solution

 We have to work out which unions of conjugacy classes are subgroups. We can start by narrowing down the possibilities to unions that include the class $A = \{e\}$ and that contain a total of 1, 2, 3, 4, 6, 8, 12 or 24 elements (since the order of S_4 is $4! = 24$). So, for example, we can dismiss $B \cup D$, as it does not include the identity element e , and we can dismiss $A \cup B$, as it contains $1 + 6 = 7$ elements. 

To draw up a list of unions of conjugacy classes that might possibly be subgroups, we need to find all the ways of adding up some of the numbers

$$1, 3, 6, 6, 8$$

(the sizes of the conjugacy classes), always including 1, to give a total of 1, 2, 3, 4, 6, 8, 12 or 24.

There is one way to obtain the total 1, namely 1 itself.

The smallest possible total greater than 1 that can be achieved with the given numbers including 1 is 4, so neither of the totals 2 or 3 is possible.

There is one way to obtain the total 4, namely $1 + 3 = 4$.

Since only one of the given numbers other than 1 is odd, namely 3, any even total must include both the numbers 1 and 3. The smallest such total that can be achieved is $1 + 3 = 4$, and adding the next smallest number, 6, gives $1 + 3 + 6 = 10$, so neither of the totals 6 and 8 is possible.

There is one way to obtain the total 12, namely $1 + 3 + 8 = 12$.

There is one way to obtain the total 24, namely $1 + 3 + 6 + 6 + 8 = 24$.



Thus there are four suitable sums of numbers:

$$1, \quad 1 + 3 = 4, \quad 1 + 3 + 8 = 12, \quad 1 + 3 + 6 + 6 + 8 = 24.$$

So the only unions of conjugacy classes that include $A = \{e\}$ and have a permissible number of elements are as follows:

$$\begin{array}{ll} A & (1 \text{ element}), \\ A \cup E & (4 \text{ elements}), \\ A \cup C \cup E & (12 \text{ elements}), \\ A \cup B \cup C \cup D \cup E & (24 \text{ elements}). \end{array}$$

If any of these sets is a subgroup, then it is a normal subgroup, by Theorem E32.

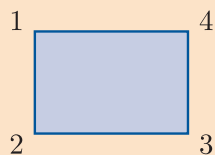
 We can use any means to determine which of these sets are subgroups. 

The first and fourth of these sets are the set $\{e\}$ and the whole set S_4 respectively, so both of these are subgroups.

The second set contains e and all the permutations in S_4 with cycle structure $(- -)(- -)$, so it is

$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

This set is the symmetry group of a rectangle with vertex locations labelled in the usual way, as shown below, so it is a subgroup.



The third set contains all the permutations in S_4 with cycle structure e , $(- - -)$ or $(- -)(- -)$, that is, all the even permutations in S_4 . Thus it is the alternating group A_4 , so it is a subgroup.

Thus the normal subgroups of S_4 are

$$\{e\}, \quad \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \quad A_4, \quad S_4.$$

The method used in Worked Exercise E32 is summarised below. Remember that the notation $|G|$, where G is a group, denotes the order of G .

Strategy E5

To find all the normal subgroups of a finite group G , do the following.

- 1. Partition G into conjugacy classes.
- 2. Find all the unions of conjugacy classes that include the class $\{e\}$ and whose total number of elements is a divisor of $|G|$.
- 3. Determine whether each such union of conjugacy classes is a subgroup of G : any union that is a subgroup is a normal subgroup of G .

In the next exercise you are asked to find all the normal subgroups of the alternating group A_5 . Before you can do this, you need to know the conjugacy classes of A_5 . Since A_5 is a subgroup of S_5 , any two elements of A_5 that are conjugate in A_5 are also conjugate in S_5 and hence have the same cycle structure. Therefore we can find the conjugacy classes of A_5 by first partitioning A_5 by cycle structure and then determining whether each cycle structure class is a conjugacy class of A_5 or whether it splits into two or more conjugacy classes. If we do this (the details are not included here), then we find that A_5 has four cycle structure classes, and only one of these splits further, into two conjugacy classes, so A_5 has five conjugacy classes. These are described in the exercise below.

Exercise E88

Given that the conjugacy classes of the alternating group A_5 are as follows, determine all the normal subgroups of A_5 .

| Conjugacy class | | Description | Number of elements |
|-----------------|-----|---|--------------------|
| A | e | | 1 |
| B | | 3-cycles | 20 |
| C | | products of two transpositions | 15 |
| D | | 5-cycles conjugate to $(1\ 2\ 3\ 4\ 5)$ | 12 |
| E | | 5-cycles conjugate to $(1\ 2\ 3\ 5\ 4)$ | 12 |

3.4 Proofs of the theorems characterising normality

Each of Theorems E28, E31 and E32, in Subsections 3.1, 3.2 and 3.3, respectively, gives a property that characterises normal subgroups. The three theorems are all summarised in the following theorem, which includes the three properties labelled as Properties B, C and D, and the property from the original definition of a normal subgroup expressed algebraically and labelled as Property A. The algebraic version of the property from the original definition was given in Proposition E13.

Theorem E33

A subgroup H of a group G is normal in G if and only if it has any one of the following equivalent properties.

- Property A** $gH = Hg$ for each $g \in G$.
- Property B** $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$.
- Property C** $gHg^{-1} = H$ for each $g \in G$.
- Property D** H is a union of conjugacy classes of G .

Although Property A was used in the original definition of a normal subgroup, any of the other three conditions could have been used in its place. We can use any of the four conditions when we wish to prove that a subgroup is normal, or show that it is not normal.

- Property A is useful when we know the partitions into left cosets and into right cosets.
- Property B is useful in many general situations.
- Property C may be helpful when we have knowledge about conjugate subgroups.
- Property D is particularly useful when we know the conjugacy classes.

As yet, you have not seen proofs of Theorems E28, E31 and E32; that is, you have not seen a proof that the four conditions are equivalent. The remainder of this subsection provides the missing proofs.

Outline of the proof

Rather than prove the three theorems individually, we will prove that if H is a subgroup of a group G , then the following five implications hold:

$$A \implies C, \quad C \implies A, \quad B \implies C, \quad C \implies D, \quad D \implies B.$$

Here A, B, C and D stand for Properties A, B, C and D, respectively.

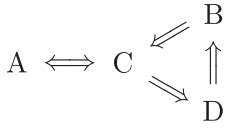


Figure 29 The five implications proved in the proof of Theorem E33

The five implications are illustrated in Figure 29. It follows from these five implications that any one of the four conditions is equivalent to any other. For example, the equivalence of conditions A and B, which we can write as $A \iff B$, follows from

$$A \implies C, \quad C \implies D, \quad D \implies B, \quad \text{which together give } A \implies B,$$

and

$$B \implies C, \quad C \implies A, \quad \text{which together give } B \implies A.$$

You may be wondering why we prove the five implications above, when we could prove Theorem E33 by proving just four implications, such as

$$A \implies B, \quad B \implies C, \quad C \implies D, \quad D \implies A.$$

The reason is that the five chosen implications are more straightforward to prove.

Proof of Theorem E33 Let H be a subgroup of a group G . We prove the five implications

$$A \implies C, \quad C \implies A, \quad B \implies C, \quad C \implies D, \quad D \implies B,$$

where A, B, C and D stand for Properties A, B, C and D, respectively.

A \implies C

Suppose that $gH = Hg$ for each $g \in G$. We have to prove that $gHg^{-1} = H$ for each $g \in G$. Let $g \in G$. Then

$$\begin{aligned} x \in gHg^{-1} & \iff x = ghg^{-1} \text{ for some } h \in H \\ & \iff x = h_1gg^{-1} \text{ for some } h_1 \in H \quad (\text{since } gH = Hg) \\ & \iff x = h_1 \text{ for some } h_1 \in H \\ & \iff x \in H, \end{aligned}$$

so $gHg^{-1} = H$, as required.

(You can check the sequence of equivalences (\iff) here by first checking all the forward implications (\implies) and then checking all the backward implications (\impliedby). The forward implications prove that $gHg^{-1} \subseteq H$, and the backward implications prove that $gHg^{-1} \supseteq H$.)

C \implies A

Suppose that $gHg^{-1} = H$ for each $g \in G$. We have to prove that $gH = Hg$ for each $g \in G$. Let $g \in G$. Then

$$\begin{aligned} x \in gH & \iff x = gh \text{ for some } h \in H \\ & \iff x = ghg^{-1}g \text{ for some } h \in H \\ & \iff x = h_1g \text{ for some } h_1 \in H \quad (\text{since } gHg^{-1} = H) \\ & \iff x \in Hg, \end{aligned}$$

so $gH = Hg$, as required.

(You can check the sequence of equivalences here in the same way as described above. The forward implications prove that $gH \subseteq Hg$, and the backward implications prove that $gH \supseteq Hg$.)

B \implies C

Suppose that $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$ (Property B). We have to prove that $gHg^{-1} = H$ for each $g \in G$. Let $g \in G$.

First we prove that $H \subseteq gHg^{-1}$. Let $h \in H$. We can write h as

$$\begin{aligned} h &= gg^{-1}hgg^{-1} \\ &= gg^{-1}h(g^{-1})^{-1}g^{-1} \quad (\text{since } g = (g^{-1})^{-1}). \end{aligned}$$

Now

$$g^{-1}h(g^{-1})^{-1} \in H,$$

by Property B, since g^{-1} is an element of G . Hence the expression for h above shows that

$$h \in gHg^{-1}.$$

Thus $H \subseteq gHg^{-1}$, as required.

It follows immediately from Property B that $gHg^{-1} \subseteq H$, so $gHg^{-1} = H$, as required.

C \implies D

Suppose that $gHg^{-1} = H$ for each $g \in G$. We have to prove that H is a union of conjugacy classes of G .

Let h be any element of H . For any element $g \in G$, we have $ghg^{-1} \in gHg^{-1}$, and hence, since $gHg^{-1} = H$, we have $ghg^{-1} \in H$. Thus H contains every conjugate in G of each of its elements; that is, H is a union of conjugacy classes of G .

D \implies B

Suppose that H is a union of conjugacy classes of G . We have to prove that $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$. For each $h \in H$ and each $g \in G$, the element ghg^{-1} lies in the conjugacy class of h and hence, since H is a union of conjugacy classes of G , it lies in H , as required.

It follows from the five implications proved above that Properties A, B, C and D are all equivalent to each other. Since by definition a subgroup H of a group G is normal in G if and only if it has Property A, this proves the theorem. ■

4 Conjugacy in symmetry groups

For some groups it is possible to say what conjugacy ‘means’ in the particular context of that group. For example, you have seen that in a symmetric group two elements are conjugate if and only if they have the same cycle structure. In this section you will see how we can interpret conjugacy in symmetry groups.

4.1 Conjugacy and geometric type

In Subsection 2.3 we found that the conjugacy classes of the symmetry group $S(\square)$ (see Figure 30) are as listed on the left below. Notice that these classes bring together symmetries of similar geometric type, as described on the right:

- | | |
|------------|---|
| $\{e\}$ | identity |
| $\{b\}$ | rotation through π |
| $\{a, c\}$ | anticlockwise and clockwise rotations through $\pi/2$ |
| $\{s, u\}$ | reflections in diagonal axes |
| $\{r, t\}$ | reflections in axes parallel to edges. |

(The rotation c is described here as a clockwise rotation through $\pi/2$ rather than as an anticlockwise rotation through $3\pi/2$ to highlight its geometric similarity to the rotation a .)

We also found in Subsection 2.3 that the conjugacy classes of the symmetry group $S(\triangle)$ (see Figure 31) are as listed on the left below. Again these classes bring together symmetries of similar geometric type, as described on the right:

- | | |
|---------------|--|
| $\{e\}$ | identity |
| $\{a, b\}$ | anticlockwise and clockwise rotations through $2\pi/3$ |
| $\{r, s, t\}$ | reflections in axes through vertices and midpoints of edges. |

As suggested by these examples, there is a link between conjugacy and geometric type in symmetry groups. To see why this is so, you need to understand what happens when you conjugate one element of a symmetry group by another. It can be quite difficult to picture this, but to try to give you some insight into it we will now look at two examples in $S(\square)$. As in Unit B1, we will track the position of the square by picturing it as a paper model coloured light blue on one side and darker blue on the other, with a dot in the same corner on both sides (as if it goes through the paper).

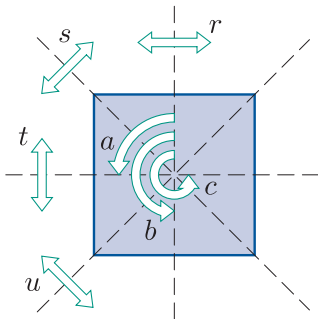


Figure 30 $S(\square)$

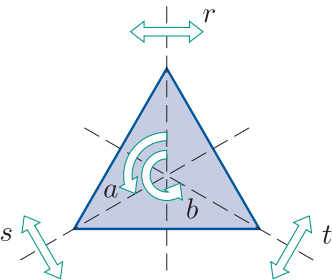


Figure 31 $S(\triangle)$

You will need to think about these examples quite carefully. If you find them hard to understand, then skip them for the moment and go on to the box headed ‘Conjugation in a symmetry group’: you should be able to apply the statement there even if you do not fully understand why it holds. Try returning to the two examples once you have completed Exercises E89 and E90.

As a first example, consider Figure 32, which shows the effect of the conjugate symmetry $r \circ a \circ r^{-1}$. To apply this conjugate symmetry, we first apply r^{-1} , which reflects the square in the vertical axis, then a , which rotates the square anticlockwise through $\pi/2$, then finally r , which ‘reflects the square back again’. Since the rotation through $\pi/2$ anticlockwise was done *when the square was in a reflected position*, the overall effect is to rotate through $\pi/2$ *clockwise*, that is to apply the symmetry c .

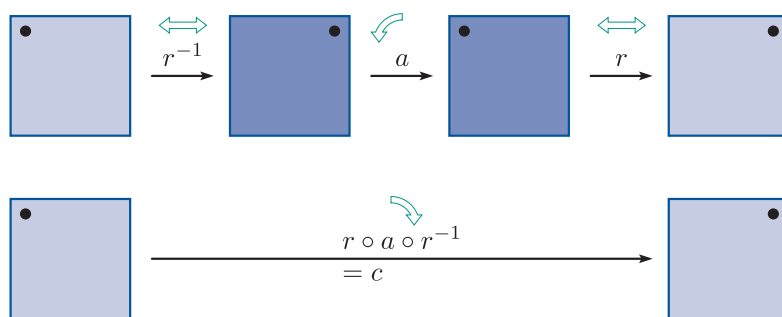


Figure 32 The effect of the conjugate symmetry $r \circ a \circ r^{-1}$ on the square

Thus the conjugate symmetry $r \circ a \circ r^{-1}$ is the symmetry obtained by ‘applying r to the *action* of a ’, as illustrated in Figure 33.

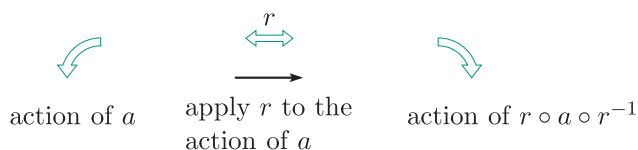


Figure 33 Conjugating a by r

(Note that here the word ‘action’ is used in its everyday sense, not in the sense of a ‘group action’, a concept that you will meet in Unit E4.)

As another example, consider Figure 34, which shows the effect of the conjugate symmetry $a \circ s \circ a^{-1}$. To apply this conjugate symmetry, we first apply a^{-1} , which rotates the square clockwise through $\pi/2$, then s , which reflects the square in the top left to bottom right diagonal axis, then finally a , which ‘rotates the square back again’. Since the reflection in the top left to bottom right axis was done *when the square was rotated clockwise by $\pi/2$* , the overall effect is to reflect in the line obtained by rotating this axis anticlockwise by $\pi/2$, which is the top right to bottom left axis – that is, the overall effect is to apply the symmetry u .

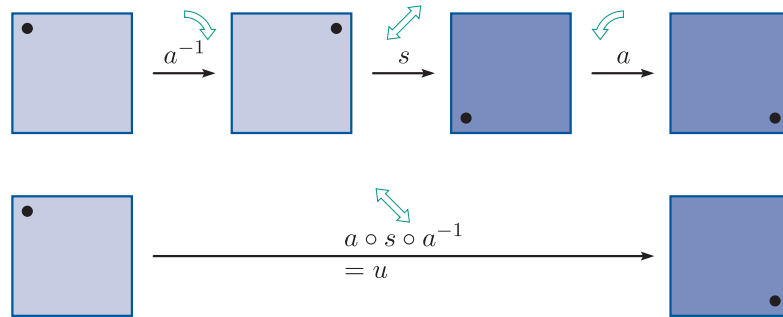


Figure 34 The effect of the conjugate symmetry $a \circ s \circ a^{-1}$ on the square

Thus the conjugate symmetry $a \circ s \circ a^{-1}$ is the symmetry obtained by ‘applying a to the *action* of s ’, as illustrated in Figure 35.

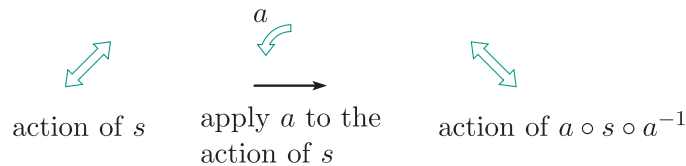


Figure 35 Conjugating s by a

In general, for any symmetries x and g of a figure F , the conjugate symmetry $g \circ x \circ g^{-1}$ is the symmetry obtained by ‘applying g to the *action* of x ’. This leads to the following helpful informal way to think about conjugacy in symmetry groups.

Conjugation in a symmetry group

Let x and g be symmetries of a figure F . Then $g \circ x \circ g^{-1}$ is the symmetry that is illustrated by the diagram obtained when g is applied to a diagram illustrating x (if we ignore any labels).

For example, in Figure 37 the symmetry r of the square (reflection in the vertical axis) is applied to a diagram for the symmetry a . By the statement in the box above, the resulting diagram illustrates the symmetry $r \circ a \circ r^{-1}$. We can see that the resulting diagram illustrates the symmetry c (see Figure 36), so $r \circ a \circ r^{-1} = c$.

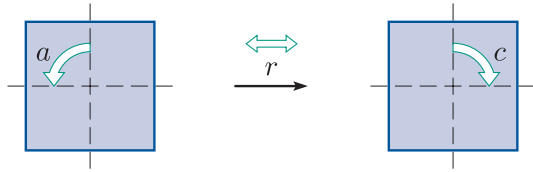


Figure 37 The conjugate symmetry $r \circ a \circ r^{-1}$ is equal to c

Similarly, in Figure 38 the symmetry a of the square (anticlockwise rotation through $\pi/2$) is applied to a diagram for the symmetry s . By the statement in the box above, the resulting diagram illustrates the symmetry $a \circ s \circ a^{-1}$. We can see that the resulting diagram illustrates the symmetry u , so $a \circ s \circ a^{-1} = u$.

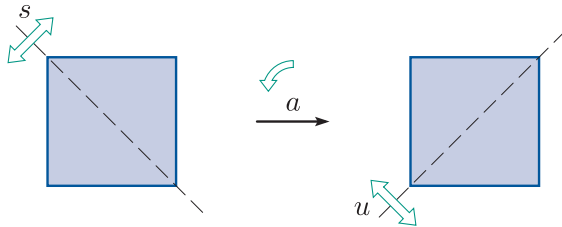


Figure 38 The conjugate symmetry $a \circ s \circ a^{-1}$ is equal to u

If two symmetries x and y are conjugate in a symmetry group, then there is often more than one symmetry that conjugates x to y .

For example, Figure 38 above illustrates that a conjugates s to u in $S(\square)$, and Figure 39 below illustrates that c (anticlockwise rotation through $3\pi/2$, or, equivalently, clockwise rotation through $\pi/2$) does the same job.

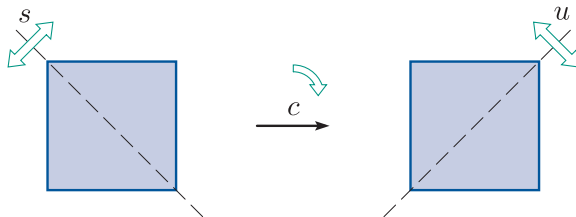


Figure 39 The conjugate symmetry $c \circ s \circ c^{-1}$ is equal to u

Figure 40 illustrates that r (reflection in the vertical axis) also does the same job.

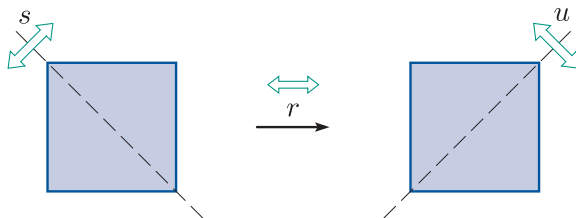


Figure 40 The conjugate symmetry $r \circ s \circ r^{-1}$ is equal to u

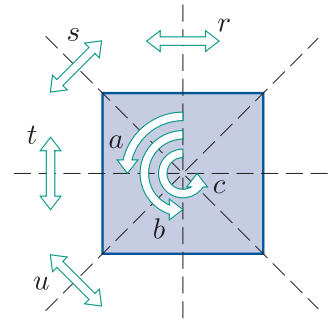


Figure 36 $S(\square)$

Make sure that you do not confuse the informal idea of a symmetry being applied to a diagram illustrating a symmetry, as in Figures 37–40, with the idea of *composing two symmetries*. For example, Figure 40 above *does not* show the symmetries s and r being composed to form the composite symmetry $r \circ s$.

The box below summarises how to use the informal ideas above to determine whether two symmetries of a figure are conjugate.

Conjugate elements in the symmetry group of a figure

- Two symmetries x and y of a figure F are conjugate in $S(F)$ if and only if there is a symmetry g of F that transforms a diagram illustrating x into a diagram illustrating y (when we ignore any labels).
- If such a symmetry g exists, then $y = g \circ x \circ g^{-1}$.

For example, Figure 37 above shows that a and c are conjugate in $S(\square)$, and Figure 38 above shows that s and u are conjugate in $S(\square)$. By way of contrast, consider the symmetries r and s in $S(\square)$ (reflection in an axis through the midpoints of opposite edges and reflection in a diagonal, respectively), as shown in Figure 41. There is no symmetry of the square that transforms a diagram illustrating r into one illustrating s , so r and s are not conjugate in $S(\square)$.

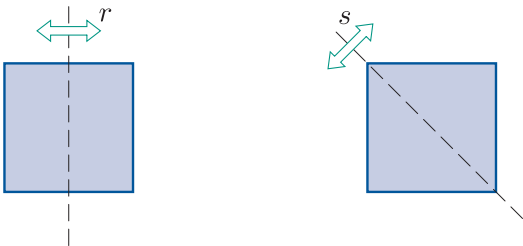


Figure 41 Diagrams illustrating the symmetries r and s of the square

Exercise E89

For each of the following pairs of symmetries in $S(\square)$ (see Figure 42), use the ideas in the box above to determine whether the two symmetries are conjugate in $S(\square)$, and to write down a symmetry that conjugates the first symmetry in the pair to the second if they are conjugate.

- (a) r and t (b) a and b (c) r and u

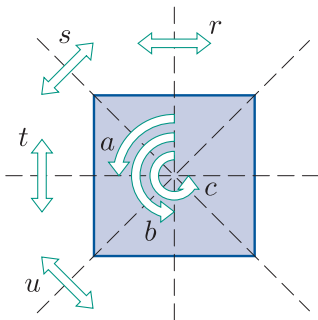
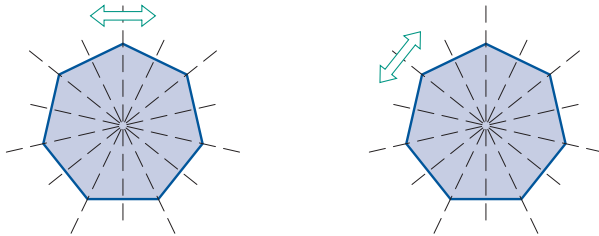


Figure 42 $S(\square)$

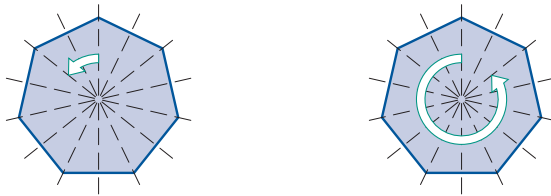
Exercise E90

For each of the following pairs of symmetries of the regular heptagon (see Figure 43), use the ideas in the box above to determine whether the two symmetries are conjugate in $S(\text{heptagon})$, and to describe a symmetry that conjugates the first symmetry in the pair to the second if they are conjugate.

- (a) Reflection in the vertical axis and reflection in the axis obtained by rotating the vertical axis by $2\pi/7$ anticlockwise.



- (b) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $12\pi/7$.



- (c) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $4\pi/7$.

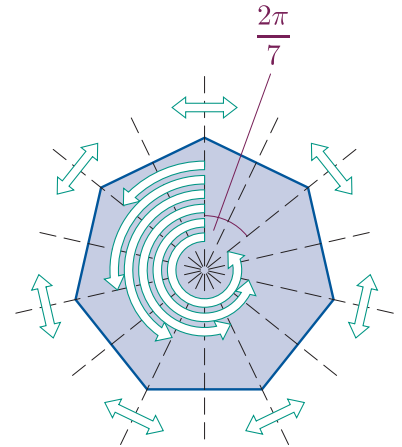
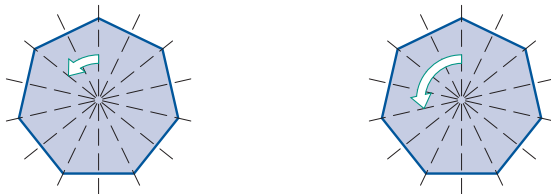


Figure 43 $S(\text{heptagon})$

The ideas in the box above explain the link between conjugacy and geometric type that you saw for $S(\square)$ and $S(\triangle)$.

These ideas apply to figures in \mathbb{R}^3 as well as to plane figures, but for such figures we have to think in terms of ‘three-dimensional diagrams’.

For example, the two reflectional symmetries x and y of the tetrahedron in Figure 44 are conjugate, because there is a rotational symmetry g of the tetrahedron (about the vertical axis) which if applied to the diagram illustrating the symmetry x gives a diagram illustrating the symmetry y .

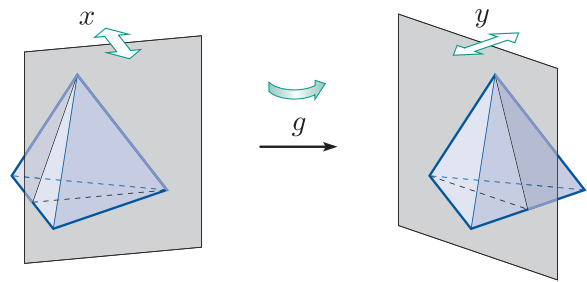


Figure 44 Two conjugate symmetries of the tetrahedron

Figure 45 may help you to understand why this is. It illustrates what happens when the symmetry x in Figure 44 is conjugated by the symmetry g mentioned above: the result is the symmetry y in Figure 44, as expected.

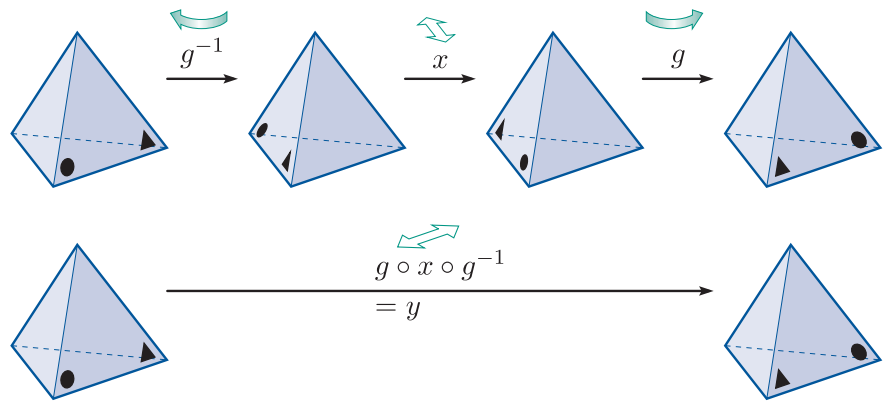


Figure 45 Two conjugate symmetries of the tetrahedron

Unfortunately it is not always practicable to determine whether symmetries of solid figures are conjugate by thinking of ‘three-dimensional diagrams’, because these diagrams can be difficult to picture: this applies particularly to indirect symmetries that are not reflections.

The ideas about the link between conjugacy and geometric type in symmetry groups that you have met so far in this subsection are expressed informally and were not proved rigorously, but we can formalise some of them by using the idea of the *fixed point set* of a symmetry of a figure. This is the set of points of the figure that are fixed – that is, not moved – by the symmetry.

Definition

Let f be a symmetry of a figure F . Then the **fixed point set** of f , denoted by $\text{Fix } f$, is given by

$$\text{Fix } f = \{P \in F : f(P) = P\}.$$

For example, the fixed point set of a non-trivial rotational symmetry of a plane figure is the centre of rotation, if this lies in the figure, and is the empty set otherwise. The fixed point set of a reflectional symmetry of a plane figure is the set of all points of the figure that lie on the axis of reflection. Figure 46 shows the fixed point sets of the rotational symmetry a and the reflectional symmetry s of the square.

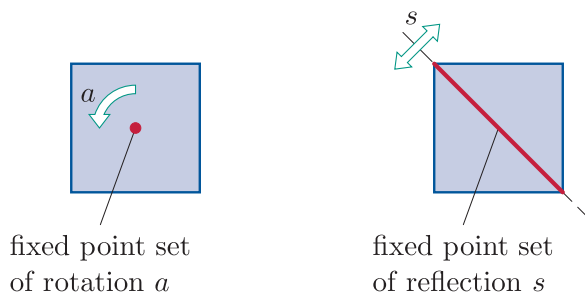


Figure 46 The fixed point sets of two symmetries of the square

Similarly, the fixed point set of a non-trivial rotational symmetry of a solid figure is the set of all points of the figure that lie on the axis of rotation. The fixed point set of a reflectional symmetry of a solid figure is the set of all points of the figure that lie in the plane of reflection. Figure 47 shows the fixed point sets of a particular rotational symmetry and a particular reflectional symmetry of the tetrahedron.

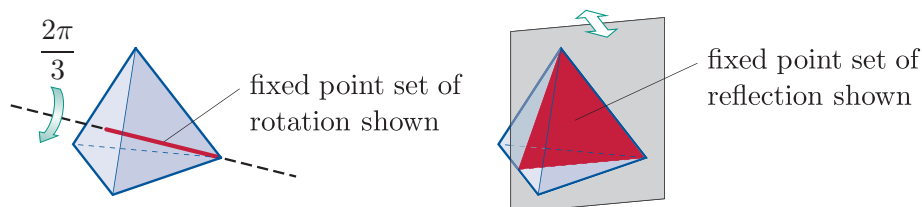
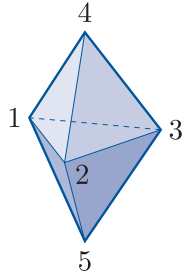


Figure 47 The fixed point sets of two symmetries of the tetrahedron

Exercise E91

Describe the fixed point set of each of the following symmetries of the double tetrahedron shown below.

- (a) The reflection in the plane through vertices 3, 4 and 5.
- (b) The reflection in the plane through vertices 1, 2 and 3.
- (c) The rotation $(1\ 2\ 3)$.



You have seen that if x and g are symmetries of a figure F , then applying g to a diagram illustrating x gives a diagram illustrating $g \circ x \circ g^{-1}$ (when we ignore any labels). So we would expect that applying g to the fixed point set of x would give the fixed point set of $g \circ x \circ g^{-1}$. This is proved formally below.

Theorem E34

Let x and g be symmetries of a figure F , and let the fixed point set of x be L . Then the fixed point set of $g \circ x \circ g^{-1}$ is $g(L)$.

Proof Throughout this proof we use the fact that if f_1 and f_2 are symmetries of F , then

$$(f_2 \circ f_1)(P) = f_2(f_1(P)) \quad \text{for each point } P \in F.$$

This is just by the definition of $f_2 \circ f_1$.

To prove the theorem we have to show that two sets are equal: $g(L)$ and the fixed point set of $g \circ x \circ g^{-1}$.

First we show that $g(L)$ is a subset of the fixed point set of $g \circ x \circ g^{-1}$. Suppose that $P \in g(L)$. Then $g^{-1}(P) \in L$. Hence $g^{-1}(P)$ is fixed by x , so

$$x(g^{-1}(P)) = g^{-1}(P).$$

Taking the image of each side of this equation under g gives

$$g(x(g^{-1}(P))) = g(g^{-1}(P)),$$

that is,

$$(g \circ x \circ g^{-1})(P) = P.$$

Thus P is in the fixed point set of $g \circ x \circ g^{-1}$. This shows that $g(L)$ is a subset of the fixed point set of $g \circ x \circ g^{-1}$.

Now we show that the fixed point set of $g \circ x \circ g^{-1}$ is a subset of $g(L)$. Suppose that P is in the fixed point set of $g \circ x \circ g^{-1}$. Then

$$(g \circ x \circ g^{-1})(P) = P.$$

Taking the image of each side of this equation under g^{-1} gives

$$g^{-1}((g \circ x \circ g^{-1})(P)) = g^{-1}(P),$$

that is,

$$x(g^{-1}(P)) = g^{-1}(P).$$

Thus $g^{-1}(P)$ is fixed by x , so $g^{-1}(P) \in L$. Hence $P \in g(L)$. This shows that the fixed point set of $g \circ x \circ g^{-1}$ is a subset of $g(L)$.

It follows that $g(L)$ is equal to the fixed point set of $g \circ x \circ g^{-1}$, as claimed. ■

By Theorem E34, if x and y are symmetries of a figure F and we want to find a symmetry g of F that conjugates x to y , then the only symmetries worth checking to see whether they do this are the symmetries that map $\text{Fix } x$ to $\text{Fix } y$ (that is, the fixed point set of x to the fixed point set of y), since any other symmetry will definitely not conjugate x to y .

Note, however, that if a symmetry g maps $\text{Fix } x$ to $\text{Fix } y$ then there is no guarantee that it conjugates x to y : it may or may not do this.

Theorem E34 tells us in particular that if there is *no* symmetry in $S(F)$ that maps $\text{Fix } x$ to $\text{Fix } y$, then x and y are not conjugate.

For example, consider the two symmetries of the tetrahedron shown in Figure 48. The fixed point set of the symmetry on the left is a line segment, whereas the fixed point set of the symmetry on the right is a triangle. Hence there is no symmetry of the tetrahedron that maps the fixed point set of the symmetry on the left to the fixed point set of the symmetry on the right. It follows by Theorem E34 that the two symmetries are not conjugate.

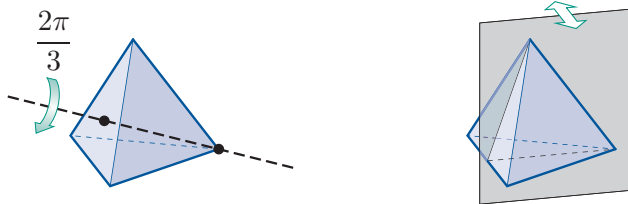


Figure 48 Two symmetries of the tetrahedron

Here is another useful result that we can sometimes apply to show that two symmetries of a figure are *not* conjugate.

Theorem E35

A direct symmetry cannot be conjugate to an indirect symmetry in a symmetry group.

Proof We use the fact that the composite of two direct symmetries or two indirect symmetries is a direct symmetry, whereas the composite of a direct symmetry and an indirect symmetry is an indirect symmetry. We also use the facts that the inverse of a direct symmetry is direct and that the inverse of an indirect symmetry is indirect.

Let x be a direct symmetry in a symmetry group and let g be any element of the group. If g is direct, then $g \circ x \circ g^{-1}$ is the composite of three direct symmetries and is therefore direct. If g is indirect, then $g \circ x \circ g^{-1}$ is the composite of a direct symmetry and two indirect symmetries and again is therefore direct. Therefore every conjugate of x is direct, which proves the theorem. ■

For example, Theorem E35 provides an even quicker method than Theorem E34 for showing that the two symmetries of the tetrahedron in Figure 48 are not conjugate. The first symmetry is a direct symmetry whereas the second symmetry is an indirect symmetry, so by Theorem E35 they are not conjugate.

4.2 Finding conjugacy classes of finite symmetry groups

In this subsection we will look at how we can find the conjugacy classes of finite symmetry groups efficiently. Remember that one reason for finding the conjugacy classes of a group is that it can help us to find its normal subgroups.

Many of the results about conjugacy that you have met can help us to work out the conjugacy classes of a symmetry group. A particularly helpful result is Proposition E26(a), from Subsection 2.3. This states that if H is a subgroup of a group G and two elements x and y of H are conjugate in H , then they must also be conjugate in G . It follows that if we represent a symmetry group $S(F)$ as a subgroup of a symmetric group S_n (by labelling the vertices of F , for example), then any symmetries that are conjugate in $S(F)$ must also be conjugate in S_n , and hence must have the same cycle structure.

So we can find the conjugacy classes of $S(F)$ by first partitioning $S(F)$ according to cycle structure, and then for each cycle structure class determining whether all the symmetries in the class are conjugate to each other or whether the class splits into two or more conjugacy classes. (Remember that the class may split because even though for any two elements x and y of $S(F)$ that have the same cycle structure there is an element g of S_n that conjugates x to y , there may not be any such element g in $S(F)$ itself.)

The strategy below sets out this approach, along with some other useful ideas.

Strategy E6

To determine the conjugacy classes of a finite symmetry group $S(F)$, do the following.

1. Represent $S(F)$ as a group of permutations.
2. Partition $S(F)$ by cycle structure.
3. For each cycle structure class, determine whether all the symmetries in the class are conjugate to each other, or whether the class splits into two or more conjugacy classes.

The following can help you do this.

- Two symmetries x and y are conjugate in $S(F)$ if and only if there is a symmetry g of F that transforms a diagram illustrating x into a diagram illustrating y .
- If x and y are conjugate in a subgroup H of $S(F)$, then they are also conjugate in $S(F)$.
- If x and y are not conjugate in a group G that has $S(F)$ as a subgroup, then they are not conjugate in $S(F)$.
- If the fixed point set of x is L , then the fixed point set of $g \circ x \circ g^{-1}$ is $g(L)$.
- A direct symmetry and an indirect symmetry are not conjugate.
- Renaming method: To find the conjugate $g \circ x \circ g^{-1}$, replace each symbol in the cycle form of x by its image under g .
- The number of elements in each conjugacy class divides $|S(F)|$.

In the next worked exercise, Strategy E6 is used to find the conjugacy classes of the symmetry group $S(\square)$ in a more efficient way than in Worked Exercise E28 in Subsection 2.3.

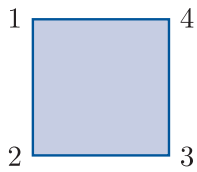


Figure 49 A labelled square

Worked Exercise E33

- (a) Express the symmetries of the square as permutations in cycle form using the usual vertex labelling, as shown in Figure 49.
- (b) Hence find the conjugacy classes of the symmetry group of the square.

Solution

- (a) The symmetries of the square are as follows.

| Rotations | Reflections |
|----------------|----------------|
| e | $(1\ 4)(2\ 3)$ |
| $(1\ 2\ 3\ 4)$ | $(2\ 4)$ |
| $(1\ 3)(2\ 4)$ | $(1\ 2)(3\ 4)$ |
| $(1\ 4\ 3\ 2)$ | $(1\ 3)$ |

- (b) To find the conjugacy classes, first partition $S(\square)$ by cycle structure.

The partition of $S(\square)$ by cycle structure is as follows.

$$\begin{aligned} &\{e\} \\ &\{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\} \\ &\{(1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\} \\ &\{(2\ 4), (1\ 3)\} \end{aligned}$$

For each cycle structure class, determine whether all the symmetries in the class are conjugate to each other, or whether the class splits into two or more conjugacy classes.

One conjugacy class is $\{e\}$.

Now consider the cycle structure class

$$\{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}.$$

The symmetries $(1\ 2\ 3\ 4)$ and $(1\ 4\ 3\ 2)$ are rotations through $\pi/2$ anticlockwise and $\pi/2$ clockwise, respectively. Hence any reflection conjugates one to the other.

As a check, we can use the reflection $(1\ 4)(2\ 3)$, say, to rename one of these symmetries and check that we obtain the other:

$$\begin{array}{c} (1\ 2\ 3\ 4) \\ (1\ 4)(2\ 3) \downarrow \downarrow \downarrow \downarrow \\ (4\ 3\ 2\ 1) = (1\ 4\ 3\ 2), \end{array}$$

as expected.

Thus this cycle structure class is a conjugacy class.

Now consider the cycle structure class

$$\{(1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}.$$

The symmetry $(1\ 3)(2\ 4)$ is not conjugate to the other two symmetries here, because it is direct whereas the other two are indirect.

The symmetries $(1\ 4)(2\ 3)$ and $(1\ 2)(3\ 4)$ are reflections in the vertical and horizontal axes, respectively. Hence a rotation through $\pi/2$ or $3\pi/2$ (anticlockwise) conjugates one to the other.

 Check:

$$\begin{array}{ccc} & (1\ 4)(2\ 3) & \\ (1\ 2\ 3\ 4) & \downarrow\downarrow\downarrow\downarrow & \\ & (2\ 1)(3\ 4) = (1\ 2)(3\ 4). & \text{cloud icon} \end{array}$$

Thus this cycle structure class splits into two conjugacy classes:

$$\{(1\ 3)(2\ 4)\}, \quad \{(1\ 4)(2\ 3), (1\ 2)(3\ 4)\}.$$

Finally, consider the cycle structure class

$$\{(2\ 4), (1\ 3)\}.$$

The symmetries $(2\ 4)$ and $(1\ 3)$ are reflections in diagonal axes. Hence a rotation through $\pi/2$ or $3\pi/2$ (anticlockwise) conjugates one to the other.


 Check:

$$\begin{array}{ccc} & (2\ 4) & \\ (1\ 2\ 3\ 4) & \downarrow\downarrow & \\ & (3\ 1) = (1\ 3). & \text{cloud icon} \end{array}$$

Thus this cycle structure class is a conjugacy class.

In summary, the conjugacy classes of $S(\square)$ are as follows.

$$\begin{aligned} &\{e\} \\ &\{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\} \\ &\{(1\ 3)(2\ 4)\} \\ &\{(1\ 4)(2\ 3), (1\ 2)(3\ 4)\} \\ &\{(2\ 4), (1\ 3)\} \end{aligned}$$

 For some purposes we may wish to rewrite these conjugacy classes with the symmetries of the square expressed as e, a, b, c, r, s, t and u instead of in cycle form. This gives the conjugacy classes as

$$\{e\}, \quad \{a, c\}, \quad \{b\}, \quad \{r, t\}, \quad \{s, u\}. \text{cloud icon}$$

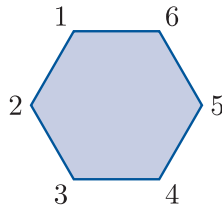
In the next two exercises, you can use Strategy E6 to find the conjugacy classes of the symmetry group $S(\triangle)$ in a more efficient way than in Exercise E77 in Subsection 2.3, and to find the conjugacy classes of the symmetry group $S(\square)$.

Exercise E92

- Express the symmetries of the equilateral triangle as permutations in cycle form using the usual vertex labelling, as shown in Figure 50.
- Hence find the conjugacy classes of the symmetry group of the equilateral triangle.

Exercise E93

- Express the symmetries of the regular hexagon below as permutations of the vertex labels in cycle form.



- Hence find the conjugacy classes of $S(\square)$, the symmetry group of the regular hexagon.
- Write down the subgroup of $S(\square)$ that is the symmetry group of the modified regular hexagon below, and use your answer to part (b) to determine whether this subgroup is normal in $S(\square)$.

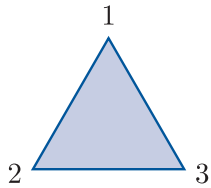
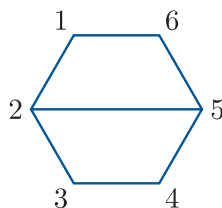
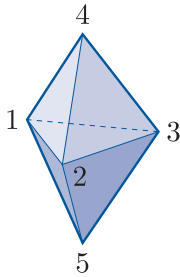


Figure 50 A labelled equilateral triangle

In the next exercise you are challenged to find the conjugacy classes of the symmetry group of the double tetrahedron. This is a little trickier than the exercises so far in this subsection, as you will probably not be able to picture three-dimensional diagrams for some of the symmetries, since some of them are not simply rotations or reflections.

Exercise E94

Consider the double tetrahedron shown below.



In Worked Exercise B39 in Subsection 2.4 of Unit B3 we found that its symmetries are as follows.

| | |
|-------------|-------------------|
| e | $(4\ 5)$ |
| $(1\ 2)$ | $(1\ 2)(4\ 5)$ |
| $(1\ 3)$ | $(1\ 3)(4\ 5)$ |
| $(2\ 3)$ | $(2\ 3)(4\ 5)$ |
| $(1\ 2\ 3)$ | $(1\ 2\ 3)(4\ 5)$ |
| $(1\ 3\ 2)$ | $(1\ 3\ 2)(4\ 5)$ |

The symmetries in the first column are the symmetries of the double tetrahedron that arise from symmetries of the equilateral triangle with vertices labelled 1, 2 and 3 in the middle of the double tetrahedron, and the symmetries in the second column are obtained by composing the symmetries in the first column with the reflectional symmetry $(4\ 5)$ of the double tetrahedron.

Find the conjugacy classes of $S(\text{doubletet})$, the symmetry group of the double tetrahedron.

Hint: Use Strategy E6. You may wish to use the fact that the symmetry group of the double tetrahedron has $S(\triangle)$ as a subgroup.

5 Conjugacy in matrix groups

In Section 2 of Unit E1 you met the group $GL(2)$, the **general linear group of degree 2**, whose elements are all the *invertible* 2×2 matrices with real entries, and whose binary operation is matrix multiplication.

You also met some subgroups of $GL(2)$, including the following standard subgroups.

- The group $SL(2)$, the **special linear group of degree 2**, whose elements are all the 2×2 matrices with determinant 1.
- The group L of all invertible 2×2 lower triangular matrices.
- The group U of all invertible 2×2 upper triangular matrices.
- The group D of all invertible 2×2 diagonal matrices.

In this section we will apply the idea of conjugacy to $GL(2)$ and some of its subgroups.

5.1 Conjugate subgroups in matrix groups

We can use the idea of conjugacy to obtain many more subgroups of $GL(2)$ than those you met in Unit E1. To do this, we apply the following theorem from Subsection 3.2.

Theorem E29

Let H be a subgroup of a group G and let g be any element of G . Then the subset gHg^{-1} is a subgroup of G .

We call the subgroup gHg^{-1} in Theorem E29 a **conjugate subgroup** of H in G .

A conjugate subgroup of a subgroup of $GL(2)$ is obtained in the worked exercise below.

Worked Exercise E34

In Exercise E21(b) in Unit E1 you saw that the following set is a subgroup of $GL(2)$:

$$P = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad = 1 \right\}.$$

(This set is specified slightly differently there.)

Find another subgroup of $GL(2)$ by conjugating P by the matrix

$$\mathbf{B} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

Solution

Apply the definition of a conjugate subgroup,

$$gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

Conjugating P by \mathbf{B} gives

$$\mathbf{B}P\mathbf{B}^{-1} = \{\mathbf{B}h\mathbf{B}^{-1} : h \in P\}$$

Replace the symbol \mathbf{B} with the matrix that it denotes, and replace the symbol h with a general element of the subgroup P .

$$= \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}^{-1} : \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in P \right\}$$

The statement $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in P$ is placing a condition on what the variables a and d can be. Simplify this condition. What it says about the variables a and d is that $a, d \in \mathbb{R}$ and $ad = 1$.

$$= \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}^{-1} : a, d \in \mathbb{R}, ad = 1 \right\}$$

Simplify the matrix product.

$$\begin{aligned} &= \left\{ \begin{pmatrix} 2a & d \\ 0 & d \end{pmatrix} \times \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} : a, d \in \mathbb{R}, ad = 1 \right\} \\ &= \left\{ \frac{1}{2} \begin{pmatrix} 2a & -2a + 2d \\ 0 & 2d \end{pmatrix} : a, d \in \mathbb{R}, ad = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & d - a \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad = 1 \right\}. \end{aligned}$$

This specification of $\mathbf{B}P\mathbf{B}^{-1}$ is acceptably simple.

It is not immediately obvious that the set specified at the end of Worked Exercise E34 is a subgroup of $\text{GL}(2)$, but by Theorem E29 we know that it is.

This subgroup is different from all the subgroups of $\text{GL}(2)$ that you have met so far in this book. However, sometimes conjugating a subgroup of $\text{GL}(2)$ by an element of $\text{GL}(2)$ can give a subgroup of $\text{GL}(2)$ that you already know about, as illustrated in the next worked exercise.

Worked Exercise E35

Consider the group U of all invertible 2×2 upper triangular matrices:

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\}.$$

- (a) Find the conjugate subgroup $\mathbf{C}U\mathbf{C}^{-1}$, where



$$\mathbf{C} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

- (b) Show that $\mathbf{C}U\mathbf{C}^{-1}$ is equal to L , the group of all invertible 2×2 lower triangular matrices.

Solution

- (a) We have

$$\begin{aligned} \mathbf{C}U\mathbf{C}^{-1} &= \{\mathbf{C}h\mathbf{C}^{-1} : h \in U\} \\ &= \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in U \right\} \\ &= \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} \\ &= \left\{ \begin{pmatrix} 0 & -d \\ a & b \end{pmatrix} \times \frac{1}{1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} \\ &= \left\{ \begin{pmatrix} d & 0 \\ -b & a \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} \end{aligned}$$

 We can write this specification in a slightly simpler way. As the value of the variable b varies through all the numbers in \mathbb{R} , so does the value of $-b$. So the specification tells us that the bottom left entry of the matrix can be any number in \mathbb{R} . Although we can specify this, as currently, by saying that the bottom left entry is $-b$, where $b \in \mathbb{R}$, it is simpler to say that the bottom left entry is b , where $b \in \mathbb{R}$. 

$$= \left\{ \begin{pmatrix} d & 0 \\ b & a \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\}.$$

- (b) The group L of all invertible 2×2 lower triangular matrices is given by

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0 \right\}.$$

The set specified here is the same as the set specified by the final line in the solution to part (a), because it does not matter whether we denote the bottom left entry by b or by c , and it does

not matter whether we denote the top left entry by d and the bottom right entry by a or vice versa, since interchanging a and d in the conditions involving a and d leaves the conditions unchanged.

Hence, by the solution to part (a) above, $\mathbf{C}U\mathbf{C}^{-1} = L$.

Exercise E95

Recall that the group D of all invertible 2×2 diagonal matrices and the group U of all invertible 2×2 upper triangular matrices are given by

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\},$$

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\}.$$

(a) Find the conjugate subgroup

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} D \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1}.$$

Is it equal to U ? Justify your answer.

(b) Find the conjugate subgroup

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} U \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}.$$

Is it equal to U ? Justify your answer.

Hint: Remember that to show that two sets are *not* equal you should show that there is an element of one set that is not an element of the other.

In Exercise E95(b) you should have found that conjugating the subgroup U of $\text{GL}(2)$ by the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

gives the subgroup U again. So in this case conjugating a subgroup of $\text{GL}(2)$ by an element of $\text{GL}(2)$ not only gives a subgroup of $\text{GL}(2)$ that we already knew about, but it gives the same subgroup that we conjugated. In the next exercise you are asked to show that this happens in two more cases.

Exercise E96

In Exercise E21(a) in Section 2 of Unit E1 you saw that the following set is a subgroup of $GL(2)$:

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

- (a) Show that conjugating M by the matrix

$$\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$$

gives the subgroup M again.

- (b) Show that conjugating M by the matrix

$$\begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}$$

gives the subgroup M again.

Exercise E96 might lead us to wonder whether conjugating the subgroup M in the exercise by *any* matrix in $GL(2)$ would give the subgroup M again. If this were true, then it would mean that the subgroup M would have the property that

$$\mathbf{B}M\mathbf{B}^{-1} = M \quad \text{for each } \mathbf{B} \in GL(2),$$

and hence, by Theorem E33 (Property C) in Subsection 3.4, M would be a normal subgroup of $GL(2)$. However, in fact it is *not* true, as is shown by the first worked exercise in the next subsection, so M is *not* a normal subgroup of $GL(2)$.

Notice, however, that both of the conjugating matrices in Exercise E96 are upper triangular matrices. It turns out that it *is* true that conjugating the subgroup M in Exercise E96 by any upper triangular matrix in $GL(2)$, that is, by any matrix in the group U , gives the subgroup M again. In other words, the subgroup M has the property that

$$\mathbf{B}M\mathbf{B}^{-1} = M \quad \text{for each } \mathbf{B} \in U.$$

Also, M is a subgroup of U , because M is a subset of U (since every matrix in M is upper triangular) and M is a group. (The relationship between the three groups M , U and $GL(2)$ is illustrated in Figure 51.) It follows by Theorem E33 (Property C) that M is a normal subgroup of U .

Thus M is a normal subgroup of U , but not a normal subgroup of $GL(2)$. This is proved in the worked exercise at the start of the next subsection, where we will use Property B of Theorem E33 rather than Property C, as this makes the proof slightly easier.

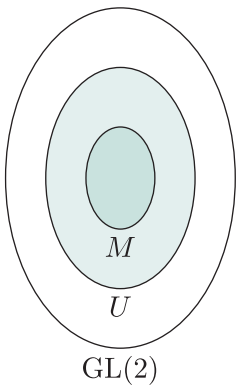


Figure 51 The relationship between the groups M , U and $GL(2)$

5.2 Normal subgroups in matrix groups

In this subsection we will look briefly at some examples of normal subgroups in matrix groups, beginning with the example mentioned at the end of the previous subsection.

We will show that subgroups are normal (or not normal) by using Property B of Theorem E33, which is restated below for convenience.

Theorem E33 (Property B)

A subgroup H of a group G is normal in G if and only if it has the following property.

Property B: $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$.

Worked Exercise E36

Consider the following subgroup of $\text{GL}(2)$, which appeared in Exercise E96:

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

The relationship between M , U and $\text{GL}(2)$ (where U is the group of all invertible 2×2 upper triangular matrices) is shown in Figure 51.

- (a) Show that M is a normal subgroup of U .
- (b) Show that M is not a normal subgroup of $\text{GL}(2)$.

Solution

- (a) We use Property B of Theorem E33.

We have to show that for every matrix $\mathbf{A} \in M$ and every matrix $\mathbf{B} \in U$, we have $\mathbf{BAB}^{-1} \in M$. Let $\mathbf{A} \in M$ and let $\mathbf{B} \in U$. Then

$$\mathbf{A} = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$$

for some $x, y, r, s, u \in \mathbb{R}$ where $x \neq 0$ and $ru \neq 0$.

We have

$$\begin{aligned} \mathbf{BAB}^{-1} &= \begin{pmatrix} r & s \\ 0 & u \end{pmatrix} \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}^{-1} \\ &= \begin{pmatrix} rx & ry + sx \\ 0 & ux \end{pmatrix} \times \frac{1}{ru} \begin{pmatrix} u & -s \\ 0 & r \end{pmatrix} \\ &= \frac{1}{ru} \begin{pmatrix} rux & -rsx + r^2y + rsx \\ 0 & rux \end{pmatrix} \\ &= \begin{pmatrix} x & ry/u \\ 0 & x \end{pmatrix}. \end{aligned}$$

☁ To check that $\mathbf{BAB}^{-1} \in M$, we have to check that it is of the form specified before the colon in the definition of M , namely

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix},$$

and also that it satisfies the conditions given after the colon, namely $a, b \in \mathbb{R}$, $a \neq 0$. ☁

This matrix is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = x$ and $b = ry/u$. Also $x \neq 0$. Hence $\mathbf{BAB}^{-1} \in M$.

Thus M is a normal subgroup of U .

(b) Again we use Property B of Theorem E33.

☁ This time we have to show that it is not satisfied. ☁

We have to show that there is a matrix $\mathbf{A} \in M$ and a matrix $\mathbf{B} \in \text{GL}(2)$ such that $\mathbf{BAB}^{-1} \notin M$.

☁ To find such matrices, we can start with a general matrix $\mathbf{A} \in M$ and a general matrix $\mathbf{B} \in \text{GL}(2)$ and proceed in a similar way to part (a) until things go wrong, as they must since M is not normal in $\text{GL}(2)$. Looking at what has gone wrong can help us find suitable matrices. Alternatively, we can try finding suitable matrices by considered experimentation. ☁

We have

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in M \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \text{GL}(2),$$

but

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}. \end{aligned}$$

This matrix is not in M since it is not an upper triangular matrix.

Hence M is not a normal subgroup of $\text{GL}(2)$.

Here are two exercises about normal subgroups of matrix groups for you to try. You can use methods similar to those used in Worked Exercise E36.

Exercise E97

Determine whether the group D of all invertible 2×2 diagonal matrices, given by

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\}$$

is a normal subgroup of $\text{GL}(2)$.

Exercise E98

(a) Show that the set

$$S = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$$

is a subgroup of $\text{GL}(2)$.

(b) Determine whether S is a normal subgroup of $\text{GL}(2)$.

(c) Determine whether S is a normal subgroup of the group U of all invertible 2×2 upper triangular matrices.

In Worked Exercise E36 at the start of this subsection you saw that the set

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}$$

is a normal subgroup of the group U of all invertible 2×2 upper triangular matrices. It follows that the quotient group U/M exists. The elements of this quotient group are the cosets of M in U . It can be shown that for every coset of M in U there is one, and only one, non-zero real number x such that the coset can be expressed as

$$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} M.$$

So there is a one-to-one correspondence between the elements of the quotient group U/M and the elements of the set \mathbb{R}^* , given by

$$\begin{aligned} \phi : U/M &\longrightarrow \mathbb{R}^* \\ \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} M &\longmapsto x. \end{aligned}$$

In fact, it can be shown that this mapping ϕ is an isomorphism, so the quotient group U/M is isomorphic to the group (\mathbb{R}^*, \times) . There is a challenging exercise in the additional exercises booklet for this unit that asks you to prove this.

Summary

In this unit you studied two important topics that are both related to normal subgroups. First you saw that we can use a normal subgroup of a group to obtain a *quotient group*, a group whose elements are the cosets of the subgroup and whose binary operation is inherited from the binary operation of the group. You saw that in this way a normal subgroup of a group can be used to ‘break down’ the group into two simpler groups, just as a positive divisor of a natural number can be used to break down the number into two simpler numbers. You went on to study *conjugacy*. You saw what this means, and how we can interpret it in symmetric groups and in symmetry groups. You also saw (particularly in the context of matrix groups) that conjugacy provides convenient ways of checking whether a subgroup of a group is normal, and ways of finding new subgroups of a group when we already have some subgroups.

Learning outcomes

After working through this unit, you should be able to:

- explain what is meant by a *quotient group*
- construct the group table of a quotient group G/N where G is a fairly small finite group and N is a normal subgroup of G
- understand the structures of the quotient groups $\mathbb{Z}/n\mathbb{Z}$, where n is an integer with $n \geq 2$, and the quotient group \mathbb{R}/\mathbb{Z}
- explain the terms *conjugate* and *conjugacy class*
- state some properties of conjugate elements
- efficiently determine the conjugacy classes of a finite group of reasonably small order
- use conjugacy to test whether a subgroup of a group is a normal subgroup
- determine conjugate subgroups of a subgroup of a finite group
- use conjugacy classes to find normal subgroups of a group
- understand and use the features of conjugacy in symmetry groups
- use conjugacy in matrix groups to find conjugate subgroups and to determine whether a subgroup is a normal subgroup.

Solutions to exercises

Solution to Exercise E49

- (a) $\{e, b\} \cdot \{r, t\} = \{e \circ r, e \circ t, b \circ r, b \circ t\}$
 $= \{r, t, t, r\}$
 $= \{r, t\}$
- (b) $\{a, c\} \cdot \{a, c\} = \{a \circ a, a \circ c, c \circ a, c \circ c\}$
 $= \{b, e, e, b\}$
 $= \{e, b\}$
- (c) $\{a, s\} \cdot \{a, s\} = \{a \circ a, a \circ s, s \circ a, s \circ s\}$
 $= \{b, t, r, e\}$
- (d) $\{a, s\} \cdot \{a, s, e\}$
 $= \{a \circ a, a \circ s, a \circ e, s \circ a, s \circ s, s \circ e\}$
 $= \{b, t, a, r, e, s\}$

Solution to Exercise E50

- (a) $\{1, 4, 7\} + \{1, 4, 7\}$
 $= \{1 +_9 1, 1 +_9 4, 1 +_9 7,$
 $4 +_9 1, 4 +_9 4, 4 +_9 7,$
 $7 +_9 1, 7 +_9 4, 7 +_9 7\}$
 $= \{2, 5, 8, 5, 8, 2, 8, 2, 5\}$
 $= \{2, 5, 8\}$
- (b) $\{0, 3, 6\} + \{1, 4, 7\}$
 $= \{0 +_9 1, 0 +_9 4, 0 +_9 7,$
 $3 +_9 1, 3 +_9 4, 3 +_9 7,$
 $6 +_9 1, 6 +_9 4, 6 +_9 7\}$
 $= \{1, 4, 7, 4, 7, 1, 7, 1, 4\}$
 $= \{1, 4, 7\}$

Solution to Exercise E51

By the solution to Worked Exercise E19(b),

$$\{b, t\} \cdot \{c, u\} = \{a, s, u, c\}.$$

Also,

$$\begin{aligned} \{c, u\} \cdot \{b, t\} &= \{c \circ b, c \circ t, u \circ b, u \circ t\} \\ &= \{a, s, s, a\} \\ &= \{a, s\}. \end{aligned}$$

Thus

$$\{b, t\} \cdot \{c, u\} \neq \{c, u\} \cdot \{b, t\}.$$

Solution to Exercise E52

(a) The Cayley table for the cosets of the normal subgroup $\{e, b\}$ of $S(\square)$ under set composition is as follows.

| \cdot | $\{e, b\}$ | $\{a, c\}$ | $\{r, t\}$ | $\{s, u\}$ |
|------------|------------|------------|------------|------------|
| $\{e, b\}$ | $\{e, b\}$ | $\{a, c\}$ | $\{r, t\}$ | $\{s, u\}$ |
| $\{a, c\}$ | $\{a, c\}$ | $\{e, b\}$ | $\{s, u\}$ | $\{r, t\}$ |
| $\{r, t\}$ | $\{r, t\}$ | $\{s, u\}$ | $\{e, b\}$ | $\{a, c\}$ |
| $\{s, u\}$ | $\{s, u\}$ | $\{r, t\}$ | $\{a, c\}$ | $\{e, b\}$ |

(b) All the sets in the body of the table are cosets of $\{e, b\}$ in $S(\square)$.

Solution to Exercise E53

(a) The Cayley table for the cosets of the normal subgroup $\{0, 3, 6\}$ of the group \mathbb{Z}_9 under set composition is as follows.

| $+$ | $\{0, 3, 6\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ |
|---------------|---------------|---------------|---------------|
| $\{0, 3, 6\}$ | $\{0, 3, 6\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ |
| $\{1, 4, 7\}$ | $\{1, 4, 7\}$ | $\{2, 5, 8\}$ | $\{0, 3, 6\}$ |
| $\{2, 5, 8\}$ | $\{2, 5, 8\}$ | $\{0, 3, 6\}$ | $\{1, 4, 7\}$ |

(b) All the sets in the body of the table are cosets of $\{0, 3, 6\}$ in \mathbb{Z}_9 .

Solution to Exercise E54

We have, for example,

$$\{a, s\} \cdot \{c, u\} = \{e, r, t, b\}.$$

This example shows that composing two left cosets of the subgroup $\{e, r\}$ in the group $S(\square)$ does not necessarily give another left coset of $\{e, r\}$. Thus the set of left cosets of $\{e, r\}$ in $S(\square)$ is not closed under set composition.

Similarly, we have

$$\{a, u\} \cdot \{c, s\} = \{e, t, r, b\}.$$

This example shows that the set of right cosets of $\{e, r\}$ in $S(\square)$ is not closed under set composition in $S(\square)$.

(There are many other counterexamples.)

Solution to Exercise E55

(Remember that $\mathbb{Z}_{17}^* = \{1, 2, \dots, 16\}$, and that the binary operation of the group \mathbb{Z}_{17}^* is \times_{17} .)

(a) In \mathbb{Z}_{17}^* we have

$$4^2 = 4 \times_{17} 4 = 16,$$

$$4^3 = 4^2 \times_{17} 4 = 16 \times_{17} 4 = 13$$

$$(\text{since } 16 \times 4 \equiv (-1) \times 4 \equiv -4 \equiv 13 \pmod{17}),$$

$$4^4 = 4^3 \times_{17} 4 = 13 \times_{17} 4 = 1$$

$$(\text{since } 13 \times 4 \equiv (-4) \times 4 \equiv -16 \equiv 1 \pmod{17}).$$

So 4 has order 4 and

$$N = \langle 4 \rangle = \{1, 4, 13, 16\}.$$

This subgroup of \mathbb{Z}_{17}^* is normal in \mathbb{Z}_{17}^* because \mathbb{Z}_{17}^* is abelian.

(b) The cosets are

$$N = \{1, 4, 13, 16\},$$

$$\begin{aligned} 2N &= \{2 \times_{17} 1, 2 \times_{17} 4, 2 \times_{17} 13, 2 \times_{17} 16\} \\ &= \{2, 8, 9, 15\}, \end{aligned}$$

$$\begin{aligned} 3N &= \{3 \times_{17} 1, 3 \times_{17} 4, 3 \times_{17} 13, 3 \times_{17} 16\} \\ &= \{3, 12, 5, 14\} \\ &= \{3, 5, 12, 14\}, \end{aligned}$$

$$\begin{aligned} 6N &= \{6 \times_{17} 1, 6 \times_{17} 4, 6 \times_{17} 13, 6 \times_{17} 16\} \\ &= \{6, 7, 10, 11\}. \end{aligned}$$

(c) The group table of \mathbb{Z}_{17}^*/N is as follows.

| \cdot | N | $2N$ | $3N$ | $6N$ |
|---------|------|------|------|------|
| N | N | $2N$ | $3N$ | $6N$ |
| $2N$ | $2N$ | N | $6N$ | $3N$ |
| $3N$ | $3N$ | $6N$ | $2N$ | N |
| $6N$ | $6N$ | $3N$ | N | $2N$ |

(The rule for composing cosets of N in \mathbb{Z}_{17}^* is

$$xN \cdot yN = (x \times_{17} y)N \quad \text{for all } x, y \in \mathbb{Z}_{17}^*.)$$

(d) The identity element of \mathbb{Z}_{17}^*/N is N . The inverses of its elements are given below.

| Element | N | $2N$ | $3N$ | $6N$ |
|---------|-----|------|------|------|
| Inverse | N | $2N$ | $6N$ | $3N$ |

(e) The group \mathbb{Z}_{17}^*/N has four elements, exactly two of which are self-inverse, so it is isomorphic to the cyclic group C_4 .

Solution to Exercise E56

(Remember that $\mathbb{Z}_{12} = \{0, 1, \dots, 11\}$, and that the binary operation of the group \mathbb{Z}_{12} is $+_{12}$.)

(a) In \mathbb{Z}_{12} we have

$$2(6) = 6 +_{12} 6 = 0,$$

so 6 has order 2 and hence $H = \langle 6 \rangle = \{0, 6\}$. This subgroup of \mathbb{Z}_{12} is normal in \mathbb{Z}_{12} because \mathbb{Z}_{12} is abelian.

(b) The cosets of H in \mathbb{Z}_{12} are

$$H = \{0, 6\},$$

$$1 + H = \{1, 7\},$$

$$2 + H = \{2, 8\},$$

$$3 + H = \{3, 9\},$$

$$4 + H = \{4, 10\},$$

$$5 + H = \{5, 11\}.$$

(c) The group table of \mathbb{Z}_{12}/H is as follows.

| $+$ | H | $1 + H$ | $2 + H$ | $3 + H$ | $4 + H$ | $5 + H$ |
|---------|---------|---------|---------|---------|---------|---------|
| H | H | $1 + H$ | $2 + H$ | $3 + H$ | $4 + H$ | $5 + H$ |
| $1 + H$ | $1 + H$ | $2 + H$ | $3 + H$ | $4 + H$ | $5 + H$ | H |
| $2 + H$ | $2 + H$ | $3 + H$ | $4 + H$ | $5 + H$ | H | $1 + H$ |
| $3 + H$ | $3 + H$ | $4 + H$ | $5 + H$ | H | $1 + H$ | $2 + H$ |
| $4 + H$ | $4 + H$ | $5 + H$ | H | $1 + H$ | $2 + H$ | $3 + H$ |
| $5 + H$ | $5 + H$ | H | $1 + H$ | $2 + H$ | $3 + H$ | $4 + H$ |

(The rule for composing cosets of H in \mathbb{Z}_{12} is

$$(x + H) + (y + H) = (x +_{12} y)H \quad \text{for all } x, y \in \mathbb{Z}_{12}.)$$

(d) The identity element of \mathbb{Z}_{12}/H is H . The inverses of its elements are given below.

| Element | H | $1 + H$ | $2 + H$ | $3 + H$ | $4 + H$ | $5 + H$ |
|---------|-----|---------|---------|---------|---------|---------|
| Inverse | H | $5 + H$ | $4 + H$ | $3 + H$ | $2 + H$ | $1 + H$ |

(e) The group \mathbb{Z}_{12}/H is abelian and has six elements, so it is isomorphic to the cyclic group C_6 .

Solution to Exercise E57

(a) The group table of G shows that $a^2 = e$, so N is the subgroup $\langle a \rangle$ of G generated by a . Also, the group table of G is symmetric with respect to the main diagonal, so G is abelian and hence N is normal in G .

(b) The cosets are

$$\begin{aligned} N &= \{e, a\}, \\ bN &= \{be, ba\} = \{b, c\}, \\ dN &= \{de, da\} = \{d, f\}, \\ gN &= \{ge, ga\} = \{g, h\}. \end{aligned}$$

(c) The group table of G/N is as follows.

| \cdot | N | bN | dN | gN |
|---------|------|------|------|------|
| N | N | bN | dN | gN |
| bN | bN | N | gN | dN |
| dN | dN | gN | N | bN |
| gN | gN | dN | bN | N |

(The rule for composing cosets of N in G is

$$xN \cdot yN = (xy)N \quad \text{for all } x, y \in G.)$$

(d) The identity element of G/N is N . Each element is self-inverse.

(e) The group G/N has four elements and each element is self-inverse, so it is isomorphic to the Klein four-group V .

(The quotient group G/N here can be spotted as a blocking of the given group table for G , as shown below.)

| | e | a | b | c | d | f | g | h |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | d | f | g | h |
| a | a | e | c | b | f | d | h | g |
| b | b | c | a | e | g | h | d | f |
| c | c | b | e | a | h | g | f | d |
| d | d | f | g | h | e | a | b | c |
| f | f | d | h | g | a | e | c | b |
| g | g | h | d | f | b | c | e | a |
| h | h | g | f | d | c | b | a | e |

Solution to Exercise E58

(a) In G we have

$$\begin{aligned} r^2 &= s, \\ r^3 &= r^2 r = sr = e. \end{aligned}$$

So r has order 3 and

$$\langle r \rangle = \{e, r, s\} = N.$$

Thus N is a subgroup of G .

Also, N has index 2 in G , so it is normal in G .

(b) The cosets are

$$\begin{aligned} N &= \{e, r, s\}, \\ pN &= \{p, q, t\}. \end{aligned}$$

(c) The group table of G/N is as follows.

| \cdot | N | pN |
|---------|------|------|
| N | N | pN |
| pN | pN | N |

(The rule for composing cosets of N in G is

$$xN \cdot yN = (xy)N \quad \text{for all } x, y \in G.)$$

(d) The identity element of G/N is N . Each element is self-inverse.

(e) The group G/N has two elements, so it is isomorphic to the cyclic group C_2 .

Solution to Exercise E59

The elements of $\mathbb{Z}/4\mathbb{Z}$ are the cosets of $4\mathbb{Z}$ in \mathbb{Z} .

The cosets are

$$\begin{aligned} 4\mathbb{Z} &= \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}, \\ 1 + 4\mathbb{Z} &= \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\}, \\ 2 + 4\mathbb{Z} &= \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\}, \\ 3 + 4\mathbb{Z} &= \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\}. \end{aligned}$$

Hence $\mathbb{Z}/4\mathbb{Z}$ has order 4.

Solution to Exercise E60

The group table of $\mathbb{Z}/4\mathbb{Z}$ is as follows.

| + | $4\mathbb{Z}$ | $1 + 4\mathbb{Z}$ | $2 + 4\mathbb{Z}$ | $3 + 4\mathbb{Z}$ |
|-------------------|-------------------|-------------------|-------------------|-------------------|
| $4\mathbb{Z}$ | $4\mathbb{Z}$ | $1 + 4\mathbb{Z}$ | $2 + 4\mathbb{Z}$ | $3 + 4\mathbb{Z}$ |
| $1 + 4\mathbb{Z}$ | $1 + 4\mathbb{Z}$ | $2 + 4\mathbb{Z}$ | $3 + 4\mathbb{Z}$ | $4\mathbb{Z}$ |
| $2 + 4\mathbb{Z}$ | $2 + 4\mathbb{Z}$ | $3 + 4\mathbb{Z}$ | $4\mathbb{Z}$ | $1 + 4\mathbb{Z}$ |
| $3 + 4\mathbb{Z}$ | $3 + 4\mathbb{Z}$ | $4\mathbb{Z}$ | $1 + 4\mathbb{Z}$ | $2 + 4\mathbb{Z}$ |

(For example,

$$(1 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = 3 + 4\mathbb{Z},$$

$$(3 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4\mathbb{Z} \quad (\text{since } 6 \in 2 + 4\mathbb{Z}),$$

$$(1 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 4 + 4\mathbb{Z} = 4\mathbb{Z} \quad (\text{since } 4 \in 4\mathbb{Z}).)$$

Solution to Exercise E61

A suitable isomorphism is

$$\begin{aligned} \phi : \mathbb{Z}/4\mathbb{Z} &\longrightarrow \mathbb{Z}_4 \\ a + 4\mathbb{Z} &\longmapsto a, \quad \text{for } a = 0, 1, 2, 3. \end{aligned}$$

Solution to Exercise E62

(a) By Theorem E16, $\mathbb{Z}/6\mathbb{Z}$ is isomorphic to \mathbb{Z}_6 and an isomorphism is

$$\begin{aligned} \phi : \mathbb{Z}/6\mathbb{Z} &\longrightarrow \mathbb{Z}_6 \\ a + 6\mathbb{Z} &\longmapsto a, \quad \text{for } a = 0, 1, 2, 3, 4, 5. \end{aligned}$$

The generators of \mathbb{Z}_6 are 1 and 5. These integers are the images under the isomorphism ϕ of the elements $1 + 6\mathbb{Z}$ and $5 + 6\mathbb{Z}$ of $\mathbb{Z}/6\mathbb{Z}$. Hence the generators of $\mathbb{Z}/6\mathbb{Z}$ are $1 + 6\mathbb{Z}$ and $5 + 6\mathbb{Z}$.

(b) The generators of \mathbb{Z}_4 are 1 and 3. So, by an argument similar to that in part (a), the generators of $\mathbb{Z}/4\mathbb{Z}$ are $1 + 4\mathbb{Z}$ and $3 + 4\mathbb{Z}$.

(c) The generators of \mathbb{Z}_5 are 1, 2, 3 and 4. So, by an argument similar to that in part (a), the generators of $\mathbb{Z}/5\mathbb{Z}$ are $1 + 5\mathbb{Z}$, $2 + 5\mathbb{Z}$, $3 + 5\mathbb{Z}$ and $4 + 5\mathbb{Z}$.

Solution to Exercise E63

(a) We have

$$\begin{aligned} 0.2 + \mathbb{Z} &= \{\dots, -1.8, -0.8, 0.2, 1.2, 2.2, 3.2, \dots\}, \\ 1.2 + \mathbb{Z} &= \{\dots, -0.8, 0.2, 1.2, 2.2, 3.2, 4.2, \dots\}, \\ 3.7 + \mathbb{Z} &= \{\dots, 1.7, 2.7, 3.7, 4.7, 5.7, 6.7, \dots\}, \\ -1.3 + \mathbb{Z} &= \{\dots, -3.3, -2.3, -1.3, \\ &\quad -0.3, 0.7, 1.7, \dots\}, \\ -4.8 + \mathbb{Z} &= \{\dots, -6.8, -5.8, -4.8, \\ &\quad -3.8, -2.8, -1.8, \dots\}. \end{aligned}$$

(b) There are only two different cosets in the list because

$$\begin{aligned} 0.2 + \mathbb{Z} &= 1.2 + \mathbb{Z} \\ &= -4.8 + \mathbb{Z} \\ &= \{\dots, -2.8, -1.8, -0.8, 0.2, 1.2, 2.2, 3.2, \dots\}, \end{aligned}$$

and

$$\begin{aligned} 3.7 + \mathbb{Z} &= -1.3 + \mathbb{Z} \\ &= \{\dots, -2.3, -1.3, -0.3, 0.7, 1.7, 2.7, 3.7, \dots\}. \end{aligned}$$

Solution to Exercise E64

(a) We have that $3.1 = 0.1 + 3$ and $0.1 \in [0, 1)$, so

$$3.1 + \mathbb{Z} = 0.1 + \mathbb{Z}.$$

(b) We have that $-0.22 = 0.78 + (-1)$ and $0.78 \in [0, 1)$, so

$$-0.22 + \mathbb{Z} = 0.78 + \mathbb{Z}.$$

(c) We have that $-3.1 = 0.9 + (-4)$ and $0.9 \in [0, 1)$, so

$$-3.1 + \mathbb{Z} = 0.9 + \mathbb{Z}.$$

Solution to Exercise E65

$$\begin{aligned} \text{(a)} \quad (0.9 + \mathbb{Z}) + (0.8 + \mathbb{Z}) &= (0.9 +_1 0.8) + \mathbb{Z} \\ &= 0.7 + \mathbb{Z} \end{aligned}$$

$$\begin{aligned} \text{(b)} \quad (0.2 + \mathbb{Z}) + \mathbb{Z} &= (0.2 + \mathbb{Z}) + (0 + \mathbb{Z}) \\ &= (0.2 +_1 0) + \mathbb{Z} \\ &= 0.2 + \mathbb{Z} \end{aligned}$$

$$\begin{aligned}
\text{(c)} \quad & (0.5 + \mathbb{Z}) + (0.7 + \mathbb{Z}) + (0.8 + \mathbb{Z}) \\
&= (0.5 +_1 0.7 +_1 0.8) + \mathbb{Z} \\
&= 0 + \mathbb{Z} \\
&= \mathbb{Z}
\end{aligned}$$

Solution to Exercise E66

(a) The element $0.25 + \mathbb{Z}$ of \mathbb{R}/\mathbb{Z} maps to the element 0.25 of the group $([0, 1), +_1)$ under the isomorphism in Theorem E17. So these two elements have the same order.

The element 0.25 of the group $([0, 1), +_1)$ has order 4, because

$$\begin{aligned}
2(0.25) &= 0.25 +_1 0.25 = 0.5, \\
3(0.25) &= 2(0.25) +_1 0.25 = 0.5 +_1 0.25 = 0.75, \\
4(0.25) &= 3(0.25) +_1 0.25 = 0.75 +_1 0.25 = 0.
\end{aligned}$$

It follows that the element $0.25 + \mathbb{Z}$ of \mathbb{R}/\mathbb{Z} also has order 4.

The cyclic subgroup generated by this element is

$$\{\mathbb{Z}, 0.25 + \mathbb{Z}, 0.5 + \mathbb{Z}, 0.75 + \mathbb{Z}\}.$$

(b) We can obtain elements with the specified orders by using the ideas of part (a).

- (i) An element of \mathbb{R}/\mathbb{Z} of order 5 is $0.2 + \mathbb{Z}$.
- (ii) An element of \mathbb{R}/\mathbb{Z} of order 2 is $0.5 + \mathbb{Z}$.
- (iii) An element of \mathbb{R}/\mathbb{Z} of order 3 is $\frac{1}{3} + \mathbb{Z}$.
- (iv) An element of \mathbb{R}/\mathbb{Z} of order 1 is the identity element \mathbb{Z} .

Solution to Exercise E67

(a) The group $S(\square)$ is not simple. The set $S^+(\square)$ of direct symmetries in $S(\square)$ is a subgroup of $S(\square)$ (by Theorem B25, which you revised in Subsection 1.4 of Unit E1), and it is normal in $S(\square)$ since it has index 2 (see Theorem E11 in Unit E1).

(b) The group \mathbb{Z}_6 is not simple. By Theorem B41 (which you revised in Subsection 3.3 of Unit E1), the subgroups of \mathbb{Z}_6 are cyclic subgroups of orders 1, 2, 3 and 6 and, since \mathbb{Z}_6 is abelian, these subgroups are all normal by Theorem E10 in Unit E1.

(c) The group \mathbb{Z}_7 is simple. By Theorem B41, the only subgroups of \mathbb{Z}_7 are cyclic subgroups of orders 1 and 7. Thus the only normal subgroups of \mathbb{Z}_7 are the trivial subgroup $\{0\}$ and \mathbb{Z}_7 .

Solution to Exercise E68

(a) (i) We use the conjugating permutation $(1\ 3\ 5)$ to rename the symbols in $(1\ 2\ 4\ 3\ 5)$:

$$\begin{array}{c}
(1\ 2\ 4\ 3\ 5) \\
(1\ 3\ 5) \downarrow \downarrow \downarrow \downarrow \downarrow \\
(3\ 2\ 4\ 5\ 1) = (1\ 3\ 2\ 4\ 5).
\end{array}$$

Thus

$$(1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (1\ 3\ 5)^{-1} = (1\ 3\ 2\ 4\ 5).$$

(ii) Using the renaming method, we obtain

$$\begin{array}{c}
(1\ 5\ 2) \\
(1\ 3)(2\ 4\ 5) \downarrow \downarrow \downarrow \\
(3\ 2\ 4) = (2\ 4\ 3).
\end{array}$$

Thus

$$(1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ ((1\ 3)(2\ 4\ 5))^{-1} = (2\ 4\ 3).$$

(b) We can check the answers to part (a) as follows.

- (i) $(1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (1\ 3\ 5)^{-1}$
 $= (1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (5\ 3\ 1)$
 $= (1\ 3\ 2\ 4\ 5)$
- (ii) $(1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ ((1\ 3)(2\ 4\ 5))^{-1}$
 $= (1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ (3\ 1)(5\ 4\ 2)$
 $= (1)(2\ 4\ 3)(5)$
 $= (2\ 4\ 3)$

Solution to Exercise E69

The permutation $(2\ 3\ 5)(4\ 6)$ can be written in the form $(- \ - \ -)(- \ -)$ in six different ways:

$$\begin{aligned}
&(2\ 3\ 5)(4\ 6), \quad (2\ 3\ 5)(6\ 4), \\
&(3\ 5\ 2)(4\ 6), \quad (3\ 5\ 2)(6\ 4), \\
&(5\ 2\ 3)(4\ 6), \quad (5\ 2\ 3)(6\ 4).
\end{aligned}$$

The conjugating permutation in Worked Exercise E24 corresponds to the middle way in the left-hand column above, and the two conjugating permutations in Worked Exercise E25 correspond to the other two ways in the left-hand column.

So we can obtain three more conjugating permutations by writing $(2\ 3\ 5)(4\ 6)$ in the three ways in the right-hand column. We obtain:

$$\begin{array}{c} (1\ 4\ 3)(2\ 6)(5) \\ g \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g = (1\ 2\ 6\ 4\ 3\ 5); \\ (2\ 3\ 5)(6\ 4)(1) \end{array}$$

$$\begin{array}{c} (1\ 4\ 3)(2\ 6)(5) \\ g \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g = (1\ 3\ 2\ 6\ 4\ 5); \\ (3\ 5\ 2)(6\ 4)(1) \end{array}$$

$$\begin{array}{c} (1\ 4\ 3)(2\ 6)(5) \\ g \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g = (1\ 5)(2\ 6\ 4). \\ (5\ 2\ 3)(6\ 4)(1) \end{array}$$

So the other three permutations in S_6 that conjugate $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$ are $(1\ 2\ 6\ 4\ 3\ 5)$, $(1\ 3\ 2\ 6\ 4\ 5)$ and $(1\ 5)(2\ 6\ 4)$.

Solution to Exercise E70

There are four ways to match up the cycles, as follows:

$$\begin{array}{c} (1\ 3)(2)(4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g = (1\ 3\ 4\ 2); \\ (3\ 4)(1)(2) \end{array}$$

$$\begin{array}{c} (1\ 3)(2)(4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g = (1\ 3\ 4); \\ (3\ 4)(2)(1) \end{array}$$

$$\begin{array}{c} (1\ 3)(2)(4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g = (1\ 4\ 2); \\ (4\ 3)(1)(2) \end{array}$$

$$\begin{array}{c} (1\ 3)(2)(4) \\ g \downarrow \downarrow \downarrow \downarrow, \text{ which gives } g = (1\ 4). \\ (4\ 3)(2)(1) \end{array}$$

So the permutations in S_4 that conjugate $(1\ 3)$ to $(3\ 4)$ are $(1\ 3\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 2)$ and $(1\ 4)$.

Solution to Exercise E71

$$(a) \ s \circ a \circ s^{-1} = s \circ (a \circ s) = s \circ r = b$$

$$(b) \ a \circ a \circ a^{-1} = a \circ (a \circ b) = a \circ e = a$$

$$(c) \ e \circ a \circ e^{-1} = e \circ (a \circ e) = e \circ a = a$$

$$(d) \ b \circ a \circ b^{-1} = b \circ (a \circ a) = b \circ b = a$$

Solution to Exercise E72

Let g be any element of G . Then, since G is abelian,

$$gxg^{-1} = xgg^{-1} = xe = x,$$

as required.

Solution to Exercise E73

$$(a) \ xex^{-1} = xx^{-1} = e$$

$$(b) \ exe^{-1} = exe = ex = x$$

Solution to Exercise E74

(a) Since $y = gxg^{-1}$, we have

$$\begin{aligned} y^2 &= gxg^{-1}gxg^{-1} \\ &= gxexg^{-1} \\ &= gx^2g^{-1}. \end{aligned}$$

(b) Since $y = gxg^{-1}$ and, by part (a), $y^2 = gx^2g^{-1}$, we have

$$\begin{aligned} y^3 &= y^2y \\ &= gx^2g^{-1}gxg^{-1} \\ &= gx^2exg^{-1} \\ &= gx^3g^{-1}. \end{aligned}$$

(c) Since $y = gxg^{-1}$ and, by part (b), $y^3 = gx^3g^{-1}$, we have

$$\begin{aligned} y^4 &= y^3y \\ &= gx^3g^{-1}gxg^{-1} \\ &= gx^3exg^{-1} \\ &= gx^4g^{-1}. \end{aligned}$$

Solution to Exercise E75

The group \mathbb{Z}_6 is abelian, so each element is conjugate to itself alone. Thus any two elements of the same order have the required property.

The orders of the elements of \mathbb{Z}_6 are as follows.

| Element | 0 | 1 | 2 | 3 | 4 | 5 |
|---------|---|---|---|---|---|---|
| Order | 1 | 6 | 3 | 2 | 3 | 6 |

The elements 1 and 5 have the same order but are not conjugate.

Similarly, the elements 2 and 4 have the same order but are not conjugate.

Solution to Exercise E76

(a) The conjugates of c in $S(\square)$ are

$$\begin{aligned} e \circ c \circ e^{-1} &= e \circ (c \circ e) = e \circ c = c, \\ a \circ c \circ a^{-1} &= a \circ (c \circ c) = a \circ b = c, \\ b \circ c \circ b^{-1} &= b \circ (c \circ b) = b \circ a = c, \\ c \circ c \circ c^{-1} &= c \circ e = c, \\ r \circ c \circ r^{-1} &= r \circ (c \circ r) = r \circ u = a, \\ s \circ c \circ s^{-1} &= s \circ (c \circ s) = s \circ r = a, \\ t \circ c \circ t^{-1} &= t \circ (c \circ t) = t \circ s = a, \\ u \circ c \circ u^{-1} &= u \circ (c \circ u) = u \circ t = a. \end{aligned}$$

The conjugacy class of c in $S(\square)$ is $\{a, c\}$.

(b) In any group, conjugating the identity element e by any other element g just gives the identity element again: $geg^{-1} = gg^{-1} = e$, as you saw in Exercise E73(a). Therefore the conjugacy class of e in $S(\square)$ is $\{e\}$.

Solution to Exercise E77

The partition of $S(\triangle)$ by the orders of its elements is

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

The set $\{e\}$ is a conjugacy class.

Consider the set $\{a, b\}$. We have

$$r \circ a \circ r^{-1} = r \circ (a \circ r) = r \circ t = b.$$

Hence $\{a, b\}$ is a conjugacy class.

Now consider the set $\{r, s, t\}$. Conjugating r by e gives r . Also,

$$a \circ r \circ a^{-1} = a \circ (r \circ b) = a \circ t = s,$$

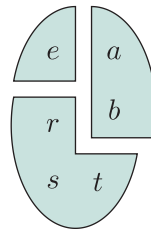
$$b \circ r \circ b^{-1} = b \circ (r \circ a) = b \circ s = t.$$

Hence $\{r, s, t\}$ is a conjugacy class.

In summary, the conjugacy classes of $S(\triangle)$ are

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

(The partition of $S(\triangle)$ into conjugacy classes is illustrated below.)



Solution to Exercise E78

We have $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

Now \mathbb{Z}_7^* is abelian and therefore each element of \mathbb{Z}_7^* is conjugate only to itself, by the result proved in Exercise E72.

Hence the partition of \mathbb{Z}_7^* into conjugacy classes is

$$\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}.$$

(Each conjugacy class contains a single element.)

Solution to Exercise E79

The group H has order 4 and is therefore abelian. So each element of H is conjugate only to itself in H .

However, all the non-identity elements of H have the same cycle structure and are therefore all conjugate to each other in S_4 .

Solution to Exercise E80

Let G be a group with identity element e . We use Theorem E28 to show that $\{e\}$ and G are normal in G .

First consider the subgroup $\{e\}$. Let h be any element of $\{e\}$, that is, $h = e$, and let g be any element of G . Then

$$ghg^{-1} = geg^{-1} = gg^{-1} = e \in \{e\}.$$

Therefore $\{e\}$ is normal in G .

Next consider the subgroup G . Let h be any element of the subgroup G and let g be any element of the group G . Then, since g , h and g^{-1} all belong to G , we have $ghg^{-1} \in G$.

Therefore G is normal in G .

Solution to Exercise E81

Let H and K be normal subgroups of a group G . Then $H \cap K$ is a subgroup of G , by Theorem B81. We use Theorem E28 to show that $H \cap K$ is normal in G .

Let x be any element of $H \cap K$ and let g be any element of G . Then x is an element of H and also an element of K , so, since both H and K are normal in G ,

$$gxg^{-1} \in H \quad \text{and} \quad gxg^{-1} \in K.$$

Hence

$$gxg^{-1} \in H \cap K.$$

Therefore $H \cap K$ is normal in G .

Solution to Exercise E82

(a) (i) Let $(a, b) \in X$. Then

$$(a, b) * (1, 0) = (a \times 1, a \times 0 + b) = (a, b).$$

(ii) Let $(a, b) \in X$. Then

$$\begin{aligned} & \left(\frac{1}{a}, -\frac{b}{a} \right) * (a, b) \\ &= \left(\frac{1}{a} \times a, \frac{1}{a} \times b + \left(-\frac{b}{a} \right) \right) \\ &= (1, 0). \end{aligned}$$

$$\begin{aligned} \text{(b) (i)} \quad & (3, 2) * (1, 7) * (3, 2)^{-1} \\ &= ((3, 2) * (1, 7)) * \left(\frac{1}{3}, -\frac{2}{3} \right) \\ &= (3, 23) * \left(\frac{1}{3}, -\frac{2}{3} \right) \\ &= (1, 21) \end{aligned}$$

$$\begin{aligned} \text{(ii)} \quad & (-1, 3) * (1, -2) * (-1, 3)^{-1} \\ &= ((-1, 3) * (1, -2)) * (-1, 3) \\ &= (-1, 5) * (-1, 3) \\ &= (1, 2) \end{aligned}$$

(c) Let $(1, b)$ be any element of A and let (c, d) be any element of X . Then $b, c, d \in \mathbb{R}$ and $c \neq 0$. We have to show that

$$(c, d) * (1, b) * (c, d)^{-1} \in A.$$

Now $(c, d)^{-1} = \left(\frac{1}{c}, -\frac{d}{c} \right)$, so we have

$$\begin{aligned} & (c, d) * (1, b) * (c, d)^{-1} \\ &= ((c, d) * (1, b)) * \left(\frac{1}{c}, -\frac{d}{c} \right) \end{aligned}$$

$$\begin{aligned} &= (c, cb + d) * \left(\frac{1}{c}, -\frac{d}{c} \right) \\ &= (1, -d + cb + d) \\ &= (1, cb). \end{aligned}$$

The element $(1, cb)$ belongs to A , since its first coordinate is 1 (and $cb \in \mathbb{R}$). Thus, by Theorem E28, A is a normal subgroup of X .

(Note that part (b) provides supporting evidence that the subgroup A is normal in X : it gives two examples of conjugates of elements of A by elements of X , both of which turn out to be elements of A .)

Solution to Exercise E83

(a) We have, for example, $(1 \ 2) \in H$ and $(1 \ 3) \in S_4$, but

$$\begin{aligned} (1 \ 3) \circ (1 \ 2) \circ (1 \ 3)^{-1} &= (3 \ 2) \\ &= (2 \ 3) \notin H. \end{aligned}$$

Therefore by Theorem E28 the subgroup H is not normal in S_4 .

(b) We have, for example, $(1 \ 3) \in H$ and $(1 \ 2) \in S_4$, but

$$(1 \ 2) \circ (1 \ 3) \circ (1 \ 2)^{-1} = (2 \ 3) \notin H.$$

Therefore by Theorem E28 the subgroup H is not normal in S_4 .

(The conjugates above can be found by using the renaming method.)

Solution to Exercise E84

First we show that K is a subgroup of X . We show that the three subgroup properties hold. (You revised these in Subsection 1.4 of Unit E1.)

SG1 Let $(1, m), (1, n) \in K$. Then $m, n \in \mathbb{Z}$. We have

$$(1, m) * (1, n) = (1, n + m).$$

This point has first coordinate 1 and its second coordinate $n + m$ is in \mathbb{Z} because $m, n \in \mathbb{Z}$. Hence it is an element of K . Thus K is closed under $*$.

SG2 The identity element of X is $(1, 0)$. This point has first coordinate 1, so it is an element of K .

SG3 Let $(1, n) \in K$. Then $n \in \mathbb{Z}$. The inverse of $(1, n)$ in X is $(1, -n)$. This point has first coordinate 1 and its second coordinate $-n$ is in \mathbb{Z} because $n \in \mathbb{Z}$. Hence it is an element of K . Thus K contains the inverse of each of its elements.

Hence K satisfies the three subgroup properties and so is a subgroup of X .

To investigate whether K is normal in X , we determine the conjugate of a general element of K by a general element of X .

Let $(1, n) \in K$ and let $(a, b) \in X$. Then $n \in \mathbb{Z}$, and $a, b \in \mathbb{R}$ with $a \neq 0$. We have

$$\begin{aligned} & (a, b) * (1, n) * (a, b)^{-1} \\ &= ((a, b) * (1, n)) * \left(\frac{1}{a}, -\frac{b}{a}\right) \\ &= (a, an + b) * \left(\frac{1}{a}, -\frac{b}{a}\right) \\ &= (1, -b + an + b) \\ &= (1, an). \end{aligned}$$

We need to determine whether this point is always an element of K . It has first coordinate 1, so to check whether it is in K we need to check whether an is always an integer. However a need not be an integer, so an will not always be an integer: for example, if $a = \frac{1}{2}$ and $n = 3$, then $an = \frac{3}{2}$. Thus $(1, an)$ will not always be in K .

So we can now give a counterexample to demonstrate that K is not a normal subgroup of X . We have $(1, 3) \in K$ and $(\frac{1}{2}, 0) \in X$, but

$$\left(\frac{1}{2}, 0\right) * (1, 3) * \left(\frac{1}{2}, 0\right)^{-1} = \left(1, \frac{3}{2}\right) \notin K.$$

Therefore by Theorem E28 the subgroup K is not normal in X .

Solution to Exercise E85

From the group table for $S(\square)$ we obtain the following.

$$\begin{aligned} \text{(a)} \quad aHa^{-1} &= \{a \circ e \circ a^{-1}, a \circ s \circ a^{-1}\} \\ &= \{e, a \circ (s \circ c)\} \\ &= \{e, a \circ t\} \\ &= \{e, u\} \end{aligned}$$

$$\begin{aligned} \text{(b)} \quad rHr^{-1} &= \{r \circ e \circ r^{-1}, r \circ b \circ r^{-1}, r \circ s \circ r^{-1}, \\ &\quad r \circ u \circ r^{-1}\} \\ &= \{e, r \circ (b \circ r), r \circ (s \circ r), r \circ (u \circ r)\} \\ &= \{e, r \circ t, r \circ a, r \circ c\} \\ &= \{e, b, u, s\} \\ &= H \end{aligned}$$

Solution to Exercise E86

(a) (i) To determine $(1\ 2\ 4)K(1\ 2\ 4)^{-1}$, we use $(1\ 2\ 4)$ to rename the symbols in each element of K .

For example, we have

$$\begin{array}{ccc} & (1\ 2)(3\ 4) & \\ (1\ 2\ 4) \downarrow \downarrow \downarrow \downarrow & & \\ & (2\ 4)(3\ 1) = (1\ 3)(2\ 4), & \end{array}$$

so the conjugate of $(1\ 2)(3\ 4)$ by $(1\ 2\ 4)$ is $(1\ 3)(2\ 4)$.

This method gives

$$\begin{aligned} & (1\ 2\ 4)K(1\ 2\ 4)^{-1} \\ &= \{e, (2\ 4)(3\ 1), (2\ 3)(4\ 1), (2\ 1)(4\ 3)\} \\ &= \{e, (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}. \end{aligned}$$

(Notice that $(1\ 2\ 4)K(1\ 2\ 4)^{-1} = K$.)

(ii) Similarly, using $(2\ 4\ 3)$ to rename the symbols in each element of K , we obtain

$$\begin{aligned} & (2\ 4\ 3)K(2\ 4\ 3)^{-1} \\ &= \{e, (1\ 4)(2\ 3), (1\ 2)(4\ 3), (1\ 3)(4\ 2)\}. \end{aligned}$$

(Notice that again $(2\ 4\ 3)K(2\ 4\ 3)^{-1} = K$.)

(b) Since conjugation does not change cycle structure, every conjugate subgroup gKg^{-1} of K in A_4 is a subgroup of A_4 of order 4 whose elements are the identity and three permutations all with cycle structure $(- -)(- -)$. However (as shown in Subsection 3.3 of Unit B3) there are only three permutations with this cycle structure in A_4 , namely the three non-identity permutations in the subgroup K . It follows that every conjugate subgroup gKg^{-1} of K in A_4 is equal to K . So K has just one conjugate subgroup, namely itself.

Solution to Exercise E87

By the solution to Exercise E77, the conjugacy classes of $S(\triangle)$ are

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

The following subgroups of $S(\triangle)$ are unions of conjugacy classes:

$$\{e\} = \{e\},$$

$$\{e, a, b\} = \{e\} \cup \{a, b\},$$

$$S(\triangle) = \{e\} \cup \{a, b\} \cup \{r, s, t\}.$$

Hence by Theorem E32 these three subgroups are normal subgroups of $S(\triangle)$.

The remaining three subgroups $\{e, r\}$, $\{e, s\}$ and $\{e, t\}$ of $S(\triangle)$ are not normal, since none of them can be expressed as a union of conjugacy classes.

Solution to Exercise E88

We apply Strategy E5.

We are given that A_5 has five conjugacy classes, and the numbers of elements in these classes are 1, 12, 12, 15 and 20.

We need to find all the unions of conjugacy classes that include the class $\{e\}$ and whose total number of elements is a divisor of $|A_5| = \frac{1}{2} \times 5! = 60$.

So we seek ways of adding some of the numbers

$$1, 12, 12, 15, 20,$$

always including 1, to obtain a total that is one of the numbers 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 or 60.

We can achieve the total 1 by taking the number 1 alone.

The smallest total greater than 1 that can be achieved with the given numbers, including 1, is $1 + 12 = 13$, so none of the totals 2, 3, 4, 5, 6, 10 and 12 is possible.

The smallest total greater than 13 that can be achieved is $1 + 15 = 16$, so the total 15 is not possible.

Since only one of the numbers other than 1 is odd, namely 15, any even total must include both the numbers 1 and 15. The smallest such totals that can be achieved are $1 + 15 = 16$, $1 + 15 + 12 = 28$

and $1 + 15 + 20 = 36$, so neither of the totals 20 and 30 is possible.

We can achieve the total 60 by adding all of the numbers.

Thus the only suitable sums of numbers are

$$1 \quad \text{and} \quad 1 + 12 + 12 + 15 + 20.$$

So the only unions of conjugacy classes that include $A = \{e\}$ and have a permissible number of elements are as follows:

$$A \quad (1 \text{ element}),$$

$$A \cup B \cup C \cup D \cup E \quad (60 \text{ elements}).$$

If either of these sets is a subgroup, then it is a normal subgroup, by Theorem E32.

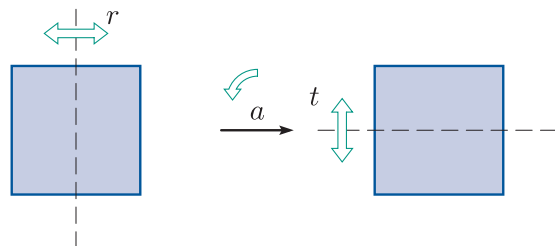
These sets are the set $\{e\}$ and the whole set A_5 respectively, so both are subgroups.

We conclude that the only normal subgroups of A_5 are the trivial subgroup $\{e\}$ and the whole group A_5 .

(The solution to this exercise shows that A_5 is a *simple* group. The definition of a simple group was given in the optional Subsection 1.3.)

Solution to Exercise E89

(a) The symmetry a transforms a diagram illustrating the symmetry r into a diagram illustrating the symmetry t , as shown below.



So the symmetry a conjugates r to t , that is,

$$t = a \circ r \circ a^{-1}.$$

Thus the symmetries r and t are conjugate in $S(\square)$.

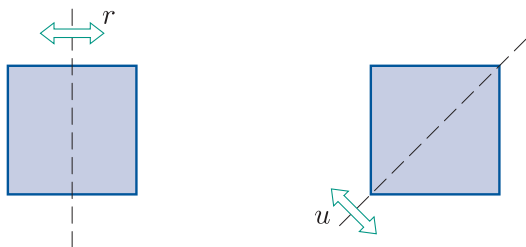
(Each of the symmetries c , s and u also transforms a diagram illustrating r into a diagram illustrating t and hence also conjugates r to t .)

(b) The symmetries a and b are shown below. There is no symmetry of the square that transforms a diagram illustrating a into a diagram illustrating b .



So there is no symmetry of the square that conjugates a to b and hence these symmetries are not conjugate in $S(\square)$.

(c) The symmetries r and u are shown below. There is no symmetry of the square that transforms a diagram illustrating r into a diagram illustrating u .

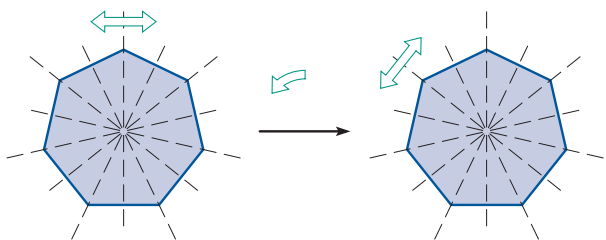


So there is no symmetry of the square that conjugates r to u and hence these symmetries are not conjugate in $S(\square)$.

Solution to Exercise E90

(a) Reflection in the vertical axis and reflection in the axis obtained by rotating the vertical axis by $2\pi/7$ anticlockwise are conjugate in $S(\text{heptagon})$.

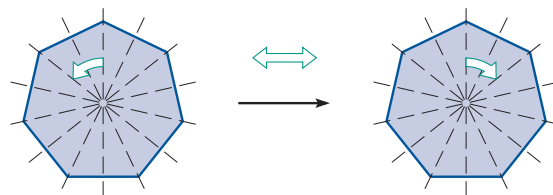
A conjugating symmetry is rotation through $2\pi/7$ anticlockwise (or reflection in the axis obtained by rotating the vertical axis by $\pi/7$ anticlockwise).



(b) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $12\pi/7$ (which is the

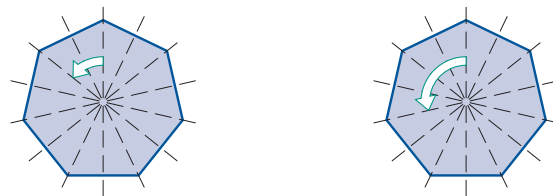
same as clockwise rotation through $2\pi/7$) are conjugate in $S(\text{heptagon})$.

A conjugating symmetry is reflection in the vertical axis (or any reflection).



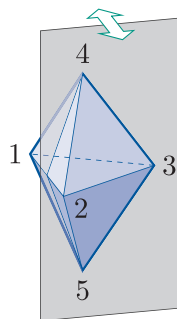
(c) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $4\pi/7$ are not conjugate in $S(\text{heptagon})$.

There is no symmetry of the heptagon that transforms a diagram illustrating the first of these symmetries into a diagram illustrating the second.



Solution to Exercise E91

(a) The fixed point set of the reflection in the plane through vertices 3, 4 and 5 is the portion of this plane that lies within the double tetrahedron, as shown below.

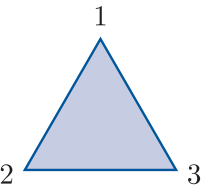


(b) The fixed point set of the reflection in the plane through vertices 1, 2 and 3 is the triangle with vertices 1, 2 and 3.

(c) The fixed point set of the rotation $(1\ 2\ 3)$ is the line segment that joins vertices 4 and 5.

Solution to Exercise E92

The labelled triangle is as follows (repeated here for convenience).



(a) The symmetries of the triangle are as follows.

| Rotations | Reflections |
|-------------|-------------|
| e | $(1\ 2)$ |
| $(1\ 2\ 3)$ | $(1\ 3)$ |
| $(1\ 3\ 2)$ | $(2\ 3)$ |

(b) The partition of $S(\triangle)$ by cycle structure is as follows.

- $\{e\}$
- $\{(1\ 2\ 3), (1\ 3\ 2)\}$
- $\{(1\ 2), (1\ 3), (2\ 3)\}$

One conjugacy class is $\{e\}$.

Now consider the cycle structure class

$$\{(1\ 2\ 3), (1\ 3\ 2)\}.$$

The symmetries $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are rotations through $2\pi/3$ anticlockwise and $2\pi/3$ clockwise, respectively. Hence any reflection conjugates one to the other. Thus this cycle structure class is a conjugacy class.

Now consider the cycle structure class

$$\{(1\ 2), (1\ 3), (2\ 3)\}.$$

The symmetry $(1\ 2\ 3)$ (rotation through $2\pi/3$ anticlockwise) transforms a diagram illustrating the symmetry $(1\ 2)$ into a diagram illustrating the symmetry $(2\ 3)$.

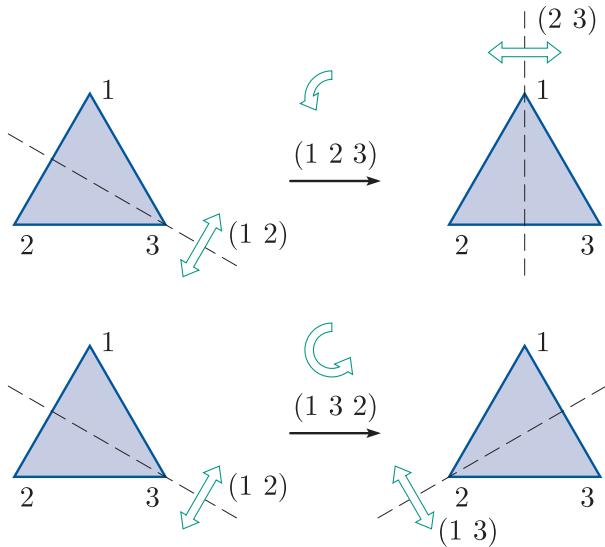
Also, the symmetry $(1\ 3\ 2)$ (rotation through $4\pi/3$ anticlockwise) transforms a diagram illustrating the symmetry $(1\ 2)$ to a diagram illustrating the symmetry $(1\ 3)$.

Hence the three symmetries in this cycle structure class are all conjugate to each other. Thus this cycle structure class is also a conjugacy class.

In summary, the conjugacy classes of $S(\triangle)$ are as follows.

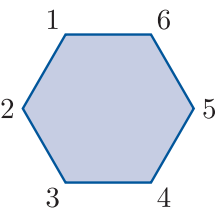
- $\{e\}$
- $\{(1\ 2\ 3), (1\ 3\ 2)\}$
- $\{(1\ 2), (1\ 3), (2\ 3)\}$

(The effects of the symmetries $(1\ 2\ 3)$ and $(1\ 3\ 2)$ mentioned above are shown below.)



Solution to Exercise E93

The labelled hexagon is as follows (repeated here for convenience).



(a) The symmetries of the hexagon are as follows.

| Rotations | Reflections |
|----------------------|----------------------|
| e | $(1\ 6)(2\ 5)(3\ 4)$ |
| $(1\ 2\ 3\ 4\ 5\ 6)$ | $(1\ 2)(3\ 6)(4\ 5)$ |
| $(1\ 3\ 5)(2\ 4\ 6)$ | $(1\ 4)(2\ 3)(5\ 6)$ |
| $(1\ 4)(2\ 5)(3\ 6)$ | $(2\ 6)(3\ 5)$ |
| $(1\ 5\ 3)(2\ 6\ 4)$ | $(1\ 3)(4\ 6)$ |
| $(1\ 6\ 5\ 4\ 3\ 2)$ | $(1\ 5)(2\ 4)$ |

(You also met the symmetries of the hexagon expressed as permutations of the vertex labels earlier in the module, in Exercise B100 in Subsection 2.4 of Unit B3.)

(b) The partition of $S(\square)$ by cycle structure is as follows.

$$\begin{aligned} &\{e\} \\ &\{(1\ 2\ 3\ 4\ 5\ 6), (1\ 6\ 5\ 4\ 3\ 2)\} \\ &\{(1\ 3\ 5)(2\ 4\ 6), (1\ 5\ 3)(2\ 6\ 4)\} \\ &\{(1\ 4)(2\ 5)(3\ 6), (1\ 6)(2\ 5)(3\ 4), \\ &\quad (1\ 2)(3\ 6)(4\ 5), (1\ 4)(2\ 3)(5\ 6)\} \\ &\{(2\ 6)(3\ 5), (1\ 3)(4\ 6), (1\ 5)(2\ 4)\} \end{aligned}$$

One conjugacy class is $\{e\}$.

Now consider the cycle structure class

$$\{(1\ 2\ 3\ 4\ 5\ 6), (1\ 6\ 5\ 4\ 3\ 2)\}.$$

The two symmetries in this class are rotations through $\pi/3$ anticlockwise and $\pi/3$ clockwise, respectively. Hence any reflection conjugates one to the other. Thus this cycle structure class is a conjugacy class.

Next consider the cycle structure class

$$\{(1\ 3\ 5)(2\ 4\ 6), (1\ 5\ 3)(2\ 6\ 4)\}.$$

The two symmetries in this class are rotations through $2\pi/3$ anticlockwise and $2\pi/3$ clockwise, respectively. Hence any reflection conjugates one to the other. Thus this cycle structure class is a conjugacy class.

Next consider the cycle structure class

$$\begin{aligned} &\{(1\ 4)(2\ 5)(3\ 6), (1\ 6)(2\ 5)(3\ 4), \\ &\quad (1\ 2)(3\ 6)(4\ 5), (1\ 4)(2\ 3)(5\ 6)\}. \end{aligned}$$

The symmetry $(1\ 4)(2\ 5)(3\ 6)$ is not conjugate to the other three symmetries here, because it is direct whereas the other three are indirect.

The three symmetries $(1\ 6)(2\ 5)(3\ 4)$, $(1\ 2)(3\ 6)(4\ 5)$ and $(1\ 4)(2\ 3)(5\ 6)$ are all reflections in axes that pass through two midpoints of edges. Hence for any pair of these symmetries there is a rotation of the hexagon that transforms a diagram illustrating one of the pair to a diagram illustrating the other. Therefore the three symmetries are all conjugate to each other.

Thus this cycle structure class splits into two conjugacy classes:

$$\begin{aligned} &\{(1\ 4)(2\ 5)(3\ 6)\}, \\ &\{(1\ 6)(2\ 5)(3\ 4), (1\ 2)(3\ 6)(4\ 5), (1\ 4)(2\ 3)(5\ 6)\}. \end{aligned}$$

Finally, consider the cycle structure class

$$\{(2\ 6)(3\ 5), (1\ 3)(4\ 6), (1\ 5)(2\ 4)\}.$$

The three symmetries in this class are all reflections in axes that pass through two vertices. Hence for any pair of these symmetries there is a rotation of the hexagon that transforms a diagram illustrating one of the pair to a diagram illustrating the other. Therefore the three symmetries are all conjugate to each other. Thus this cycle structure class is a conjugacy class.

In summary, the conjugacy classes of $S(\square)$ are as follows.

$$\begin{aligned} &\{e\} \\ &\{(1\ 2\ 3\ 4\ 5\ 6), (1\ 6\ 5\ 4\ 3\ 2)\} \\ &\{(1\ 3\ 5)(2\ 4\ 6), (1\ 5\ 3)(2\ 6\ 4)\} \\ &\{(1\ 4)(2\ 5)(3\ 6)\} \\ &\{(1\ 6)(2\ 5)(3\ 4), (1\ 2)(3\ 6)(4\ 5), (1\ 4)(2\ 3)(5\ 6)\} \\ &\{(2\ 6)(3\ 5), (1\ 3)(4\ 6), (1\ 5)(2\ 4)\} \end{aligned}$$

(c) The symmetry group of the given modified regular hexagon is

$$\{e, (1\ 6)(2\ 5)(3\ 4), (1\ 3)(4\ 6), (1\ 4)(2\ 5)(3\ 6)\}.$$

This subgroup is not normal in $S(\square)$ because it is not a union of conjugacy classes of $S(\square)$. For example, the element $(1\ 3)(4\ 6)$ of the subgroup lies in the same conjugacy class as $(1\ 5)(2\ 4)$, but this symmetry is not an element of the subgroup.

Solution to Exercise E94

We use Strategy E6. There are many different ways to work out the conjugacy classes of $S(\text{doubletet})$. One method is given here.

The partition of $S(\text{doubletet})$ by cycle structure is as follows.

$$\begin{aligned} &\{e\} \\ &\{(1\ 2), (1\ 3), (2\ 3), (4\ 5)\} \\ &\{(1\ 2\ 3), (1\ 3\ 2)\} \\ &\{(1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5)\} \\ &\{(1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\} \end{aligned}$$

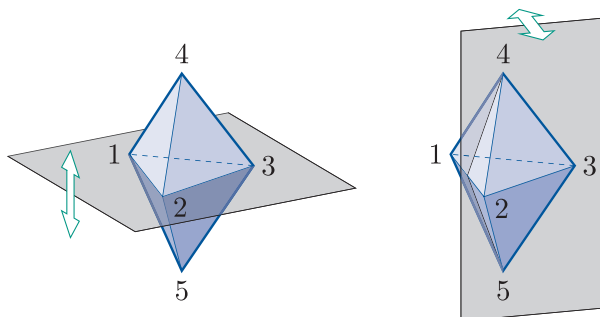
One conjugacy class is $\{e\}$.

Now consider the cycle structure class

$$\{(1\ 2), (1\ 3), (2\ 3), (4\ 5)\}.$$

We can use the fact that the group $S(\triangle)$, with its usual representation as permutations of the vertex labels 1, 2 and 3, is a subgroup of $S(\text{doubletet})$. The elements $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ are all conjugate in $S(\triangle)$ (by the solution to Exercise E92), so they are all conjugate in $S(\text{doubletet})$.

The symmetry $(4\ 5)$ is the reflection in the plane passing through the vertices 1, 2 and 3, shown on the left below. Its fixed point set is the triangle with vertices 1, 2 and 3. The symmetry $(1\ 2)$ is the reflection in the plane passing through the vertices 3, 4 and 5, shown on the right below. Its fixed point set is the part of this plane lying within the double tetrahedron. There is no symmetry of the double tetrahedron that maps one of these two fixed point sets to the other, so by Theorem E34 the symmetries $(4\ 5)$ and $(1\ 2)$ are not conjugate in $S(\text{doubletet})$.



Thus the cycle structure class above splits into two conjugacy classes:

$$\{(1\ 2), (1\ 3), (2\ 3)\}, \quad \{(4\ 5)\}.$$

Next consider the cycle structure class

$$\{(1\ 2\ 3), (1\ 3\ 2)\}.$$

Similarly to the above, the two elements of this class are conjugate in $S(\triangle)$, so they are also conjugate in $S(\text{doubletet})$. Thus this cycle structure class is a conjugacy class.

Now consider the cycle structure class

$$\{(1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5)\}.$$

We know that in $S(\triangle)$ the element $(1\ 2\ 3)$ conjugates $(1\ 2)$ to $(2\ 3)$, so in $S(\text{doubletet})$ it must conjugate $(1\ 2)(4\ 5)$ to $(2\ 3)(4\ 5)$, since it will have no effect on the cycle $(4\ 5)$:

$$\begin{array}{c} (1\ 2)(4\ 5) \\ (1\ 2\ 3) \downarrow \downarrow \downarrow \downarrow \\ (2\ 3)(4\ 5). \end{array}$$

Similarly, in $S(\triangle)$ the element $(1\ 2\ 3)$ conjugates $(2\ 3)$ to $(1\ 3)$, so in $S(\text{doubletet})$ it must conjugate $(2\ 3)(4\ 5)$ to $(1\ 3)(4\ 5)$:

$$\begin{array}{c} (2\ 3)(4\ 5) \\ (1\ 2\ 3) \downarrow \downarrow \downarrow \downarrow \\ (3\ 1)(4\ 5) = (1\ 3)(4\ 5). \end{array}$$

Thus the cycle structure class above is a conjugacy class.

Finally consider the cycle structure class

$$\{(1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\}.$$

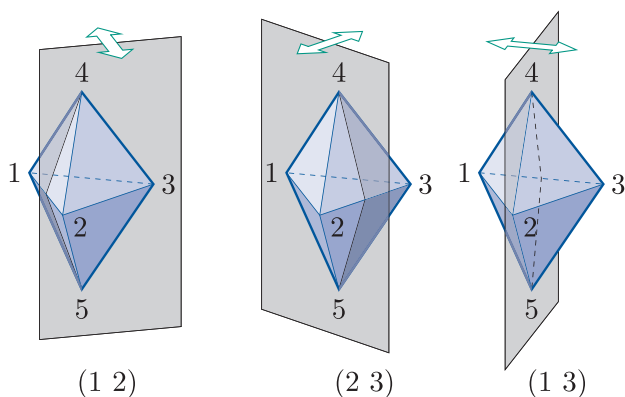
We can argue in a similar way as for the previous cycle structure class. We know that in $S(\triangle)$ the element $(2\ 3)$ conjugates $(1\ 2\ 3)$ to $(1\ 3\ 2)$, so in $S(\text{doubletet})$ it must conjugate $(1\ 2\ 3)(4\ 5)$ to $(1\ 3\ 2)(4\ 5)$. Thus this cycle structure class is a conjugacy class.

In summary, the conjugacy classes of $S(\text{doubletet})$ are as follows.

$$\begin{aligned} &\{e\} \\ &\{(1\ 2), (1\ 3), (2\ 3)\} \\ &\{(4\ 5)\} \\ &\{(1\ 2\ 3), (1\ 3\ 2)\} \\ &\{(1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5)\} \\ &\{(1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\} \end{aligned}$$

(Here are some alternative methods that you could have used.

To work out that the three symmetries $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ are all conjugate, you can consider the geometric effects of these symmetries. They are all reflections in vertical planes, as shown below.



We would expect from these diagrams, or by considering the fixed point sets of these symmetries, that the rotation $(1\ 2\ 3)$ would conjugate $(1\ 2)$ to $(2\ 3)$ and conjugate $(2\ 3)$ to $(1\ 3)$, and we can confirm this by using the renaming method:

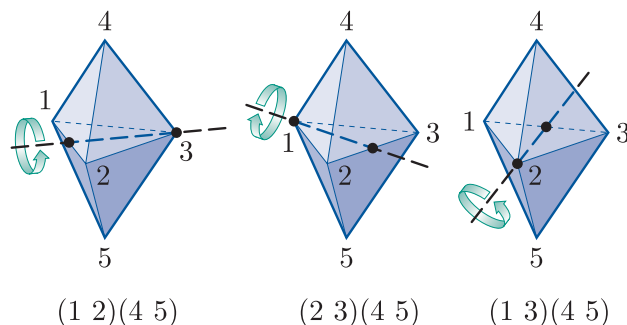
$$\begin{array}{ccc} (1\ 2) & & (2\ 3) \\ (1\ 2\ 3) \downarrow \downarrow & & (1\ 2\ 3) \downarrow \downarrow \\ (2\ 3), & & (3\ 1) = (1\ 3). \end{array}$$

Thus the three symmetries $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ are all conjugate.

To work out that the cycle structure class

$$\{(1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5)\}$$

is a conjugacy class, again we can consider the effects of these symmetries. Each of them is a rotation through π about a horizontal axis, as shown below.



We would expect from these diagrams, or by considering the fixed point sets of these symmetries, that the rotation $(1\ 2\ 3)$ would conjugate $(1\ 2)(4\ 5)$ to $(2\ 3)(4\ 5)$ and conjugate $(2\ 3)(4\ 5)$ to $(1\ 3)(4\ 5)$, and we can confirm this using the renaming method, as is done in the main solution above.

To work out that the cycle structure class

$$\{(1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\}$$

is a conjugacy class, we can simply try conjugating the symmetry $(1\ 2\ 3)(4\ 5)$ by elements of $S(\text{doubletet})$ in turn (using the renaming method) to see if we can obtain the symmetry $(1\ 3\ 2)(4\ 5)$. It does not take long to find a suitable conjugating symmetry, as any of the symmetries $(1\ 2)$, $(1\ 3)$, $(2\ 3)$, $(1\ 2)(4\ 5)$, $(1\ 3)(4\ 5)$ and $(2\ 3)(4\ 5)$ will do. Note that finding the fixed point sets of the symmetries $(1\ 2\ 3)(4\ 5)$ and $(1\ 3\ 2)(4\ 5)$ is of no help, as the fixed point set of each of these two symmetries consists of the central point of the double tetrahedron alone, so every symmetry of the double tetrahedron maps the fixed point set of the first symmetry to the fixed point set of the second.)

Solution to Exercise E95

(a) We have

$$\begin{aligned}
& \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} D \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1} \\
&= \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1} : \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in D \right\} \\
&= \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1} : a, d \in \mathbb{R}, ad \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & 2d \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & -2a + 2d \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\}.
\end{aligned}$$

This subgroup is not equal to U because, for example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in U,$$

since this matrix is upper triangular and invertible, but

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \notin \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} D \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1},$$

because there are no numbers $a, d \in \mathbb{R}$ such that

$$\begin{pmatrix} a & -2a + 2d \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

This is because if $a = 1$ and $d = 2$ then

$$-2a + 2d = 2 \neq 0.$$

(b) We have

$$\begin{aligned}
& \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} U \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \\
&= \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in U \right\} \\
&= \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & b + d \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & -a + b + d \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & c \\ 0 & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0 \right\}.
\end{aligned}$$

The final line in the manipulation above is correct because as the value of b varies through all the numbers in \mathbb{R} , so does the value of $-a + b + d$, so we can denote the top right entry simply by c , say, where $c \in \mathbb{R}$.

(Alternatively we could denote the top right entry by b , where $b \in \mathbb{R}$, but using a different variable may help to make the argument clearer.)

This subgroup is equal to U because the specification found above is exactly the same as the specification for U , except that the top right entry of the matrix is denoted by c instead of b , which does not make any difference to the set specified.

Solution to Exercise E96

(a) We have

$$\begin{aligned}
& \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} M \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}^{-1} \\
&= \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}^{-1} : \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M \right\} \\
&= \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}^{-1} : a, b \in \mathbb{R}, a \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & b + 3a \\ 0 & 2a \end{pmatrix} \times \frac{1}{2} \begin{pmatrix} 2 & -3 \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\} \\
&= \left\{ \frac{1}{2} \begin{pmatrix} 2a & b \\ 0 & 2a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & \frac{1}{2}b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & c \\ 0 & a \end{pmatrix} : a, c \in \mathbb{R}, a \neq 0 \right\}.
\end{aligned}$$

The final line in the manipulation above is correct because as the value of b varies through all the numbers in \mathbb{R} , so does the value of $\frac{1}{2}b$, so we can denote the top right entry simply by c , say, where $c \in \mathbb{R}$.

(Alternatively we could denote the top right entry by b , where $b \in \mathbb{R}$.)

This subgroup is equal to M because the specification found above is exactly the same as the specification for M , except that the top right entry of the matrix is denoted by c instead of b , which does not make any difference to the set specified.

(b) We have

$$\begin{aligned}
 & \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix} M \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}^{-1} \\
 &= \left\{ \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}^{-1} : \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M \right\} \\
 &= \left\{ \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}^{-1} : a, b \in \mathbb{R}, a \neq 0 \right\} \\
 &= \left\{ \begin{pmatrix} 2a & 2b-3a \\ 0 & -a \end{pmatrix} \times \begin{pmatrix} -1 \\ -2 \end{pmatrix} \begin{pmatrix} -1 & 3 \\ 0 & 2 \end{pmatrix} : \right. \\
 &\quad \left. a, b \in \mathbb{R}, a \neq 0 \right\} \\
 &= \left\{ -\frac{1}{2} \begin{pmatrix} -2a & 4b \\ 0 & -2a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\} \\
 &= \left\{ \begin{pmatrix} a & -2b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\} \\
 &= \left\{ \begin{pmatrix} a & c \\ 0 & a \end{pmatrix} : a, c \in \mathbb{R}, a \neq 0 \right\}.
 \end{aligned}$$

The final line in the manipulation above is correct because as the value of b varies through all the numbers in \mathbb{R} , so does the value of $-2b$, so we can denote the top right entry simply by c , say, where $c \in \mathbb{R}$.

(Alternatively we could denote the top right entry by b , where $b \in \mathbb{R}$.)

As in part (a), this subgroup is equal to M because the specification found above is exactly the same as the specification for M , except that the top right entry of the matrix is denoted by c instead of b , which does not make any difference to the set specified.

Solution to Exercise E97

We use Property B of Theorem E33.

The subgroup D is not a normal subgroup of $\text{GL}(2)$, because, for example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in D \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \text{GL}(2),$$

but

$$\begin{aligned}
 & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \\
 &= \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix},
 \end{aligned}$$

which is not in D since it is not a diagonal matrix.

Solution to Exercise E98

(a) The set S is a *subset* of the group $\text{GL}(2)$, because each matrix

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

in S has determinant

$$1 \times 1 - b \times 0 = 1$$

and is therefore invertible.

We show that the three subgroup properties hold for S (with the same binary operation as in $\text{GL}(2)$, namely matrix multiplication).

SG1 Closure

Let $\mathbf{A}, \mathbf{B} \in S$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix},$$

for some $x, y \in \mathbb{R}$. So

$$\mathbf{AB} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}.$$

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with

$b = x + y \in \mathbb{R}$. So $\mathbf{AB} \in S$. Thus S is closed under matrix multiplication.

SG2 Identity

The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of $\text{GL}(2)$ is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = 0$.

Thus $\mathbf{I} \in S$.

SG3 Inverses

Let $\mathbf{A} \in S$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

for some $x \in \mathbb{R}$. The inverse of \mathbf{A} in $\text{GL}(2)$ is

$$\mathbf{A}^{-1} = \frac{1}{1} \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}.$$

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with

$b = -x \in \mathbb{R}$. So $\mathbf{A}^{-1} \in S$. Thus S contains the inverse of each of its elements.

Since the three subgroup properties hold, S is a subgroup of $\text{GL}(2)$.

(This solution is similar to the solution to Worked Exercise E8 in Section 2 of Unit E1. The subset Y of $\text{GL}(2)$ defined there and the subset S of $\text{GL}(2)$ defined here have similar – but not the same – definitions.)

(b) We use Property B of Theorem E33.

The subgroup S is not a normal subgroup of $\text{GL}(2)$, because, for example,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in S \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \text{GL}(2),$$

but

$$\begin{aligned} & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \end{aligned}$$

which is not in S since (for example) its bottom right entry is not 1.

(c) The set S is a subset of the group U , because each matrix in it is upper triangular and has determinant 1 so is invertible. Also, S is a group under matrix multiplication, by part (a). Therefore S is a subgroup of U .

To show that S is normal in U , we use Property B of Theorem E33.

We have to show that for every matrix $\mathbf{A} \in S$ and every matrix $\mathbf{B} \in U$, we have $\mathbf{BAB}^{-1} \in S$. Let $\mathbf{A} \in S$ and let $\mathbf{B} \in U$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$$

for some $x, r, s, u \in \mathbb{R}$ where $ru \neq 0$.

We have

$$\begin{aligned} \mathbf{BAB}^{-1} &= \begin{pmatrix} r & s \\ 0 & u \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}^{-1} \\ &= \begin{pmatrix} r & rx+s \\ 0 & u \end{pmatrix} \times \frac{1}{ru} \begin{pmatrix} u & -s \\ 0 & r \end{pmatrix} \\ &= \frac{1}{ru} \begin{pmatrix} ru & -rs+rxu+rs \\ 0 & ru \end{pmatrix} \\ &= \begin{pmatrix} 1 & rx/u \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

This matrix is of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

with $b = rx/u \in \mathbb{R}$. Hence $\mathbf{BAB}^{-1} \in S$.

Thus S is a normal subgroup of U .

Unit E3

Homomorphisms

Introduction

In this unit you will study mappings whose domains and codomains are groups, and that (in a sense that you will learn about) preserve some of the structure of their domain groups. Such mappings are called *homomorphisms*. A homomorphism can provide insight into the relationship between the groups that are its domain and codomain.

You have already met many examples of homomorphisms in this module, because every isomorphism is a homomorphism – one that preserves *all* the structure of the domain group.

You will study some properties common to all homomorphisms, and meet the ideas of the *image* and *kernel* of a homomorphism, which are similar to the *image set* and *kernel* of a linear transformation (you met these ideas in Book C *Linear algebra*). The final section of the unit introduces you to one of the most important theorems in the group theory units: the *First Isomorphism Theorem*. This theorem brings together the idea of homomorphisms with many other concepts in group theory that you have already met – in particular, normal subgroups and quotient groups.

1 Isomorphisms and homomorphisms

In this section you will start by looking again at *isomorphisms*, concentrating on features that will be important in this unit. You will go on to learn what a homomorphism is, meet some examples of homomorphisms and study some of their properties.

For clarity, throughout this section and throughout the rest of this unit we will mostly *not* use concise multiplicative notation for abstract groups – instead we will use symbols for their binary operations. This is because we will usually be dealing with two groups at the same time – a domain group and a codomain group of a mapping – each with its own binary operation.

1.1 Isomorphisms

You met the ideas of *isomorphic groups* and *isomorphisms* in Unit B2 *Subgroups and isomorphisms*, and revised them briefly in Unit E1 *Cosets and normal subgroups*. You saw that two groups are *isomorphic* if they have identical structures – that is, if one of the groups can be obtained from the other by ‘renaming’ the elements (and the binary operation). A mapping from one of the groups to the other that carries out such a renaming of the elements is called an *isomorphism*. Remember that ‘mapping’ is just another name for ‘function’: it is often the preferred term in group theory and other algebraic areas of mathematics.

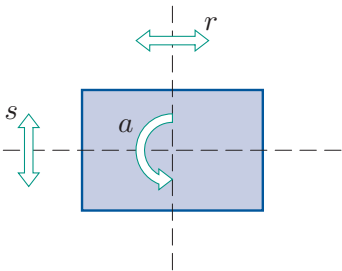


Figure 1 $S(\square)$

Until now our main interest when dealing with isomorphisms has been in whether or not two groups are isomorphic, but in this subsection our primary interest is in the isomorphisms themselves. We will start with another brief revision of the ideas of isomorphic groups and isomorphisms from this perspective.

Consider the two groups

- $(S(\square), \circ)$, the group of symmetries of the rectangle (see Figure 1)
- (U_8, \times_8) , the group of integers in \mathbb{Z}_8 coprime to 8 under multiplication modulo 8.

Their group tables are as follows.

| \circ | e | a | r | s |
|---------|-----|-----|-----|-----|
| e | e | a | r | s |
| a | a | e | s | r |
| r | r | s | e | a |
| s | s | r | a | e |

$(S(\square), \circ)$

| \times_8 | 1 | 3 | 5 | 7 |
|------------|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

(U_8, \times_8)

If we replace each entry in the group table of $(S(\square), \circ)$ by its image under the mapping

$$\begin{aligned}\phi : (S(\square), \circ) &\longrightarrow (U_8, \times_8) \\ e &\longmapsto 1 \\ a &\longmapsto 3 \\ r &\longmapsto 5 \\ s &\longmapsto 7\end{aligned}$$

(and replace the symbol \circ at the top left by \times_8), then we obtain the group table of (U_8, \times_8) .

Since the mapping ϕ transforms the group table of $(S(\square), \circ)$ into a group table for (U_8, \times_8) , it is an isomorphism and the two groups are isomorphic.

Notice that the first line of the specification for the mapping ϕ above is given as

$$\phi : (S(\square), \circ) \longrightarrow (U_8, \times_8)$$

rather than just

$$\phi : S(\square) \longrightarrow U_8.$$

When we discuss mappings between groups we often include the binary operations in this way, for clarity. However, as always, we can omit them if they are clear from the context.

There is usually more than one isomorphism between two isomorphic groups. For example, consider the mapping

$$\begin{aligned}\phi_1 : (S(\square), \circ) &\longrightarrow (U_8, \times_8) \\ e &\longmapsto 1 \\ a &\longmapsto 5 \\ r &\longmapsto 7 \\ s &\longmapsto 3.\end{aligned}$$

If we replace each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_1 , then we obtain the following table.

| | 1 | 5 | 7 | 3 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 3 |
| 5 | 5 | 1 | 3 | 7 |
| 7 | 7 | 3 | 1 | 5 |
| 3 | 3 | 7 | 5 | 1 |

Although this is not the group table of (U_8, \times_8) that was given above, it is *a* group table of (U_8, \times_8) . The entries in the borders of the table are in a different order, but the entries in the body of the table have been rearranged accordingly. Thus ϕ_1 is also an isomorphism from $(S(\square), \circ)$ to (U_8, \times_8) .

An isomorphism from one group to another must be a one-to-one and onto mapping, of course – that is, it must match up each element of one group with exactly one element of the other group and vice versa, as illustrated in Figure 2.

However, even if two groups are isomorphic, not every one-to-one and onto mapping from one of the groups to the other group is an isomorphism. For example, consider the mapping

$$\begin{aligned}\phi_2 : (S(\square), \circ) &\longrightarrow (U_8, \times_8) \\ e &\longmapsto 3 \\ a &\longmapsto 1 \\ r &\longmapsto 5 \\ s &\longmapsto 7.\end{aligned}$$

If we replace each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_2 , then we obtain the following table.

| | 3 | 1 | 5 | 7 |
|---|---|---|---|---|
| 3 | 3 | 1 | 5 | 7 |
| 1 | 1 | 3 | 7 | 5 |
| 5 | 5 | 7 | 3 | 1 |
| 7 | 7 | 5 | 1 | 3 |

This is not a group table of (U_8, \times_8) , because, for example, it is not true that $3 \times_8 3 = 3$. So ϕ_2 is not an isomorphism.

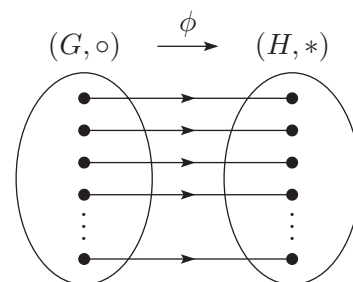


Figure 2 A one-to-one and onto mapping between two groups

Exercise E99

The group tables for the groups $(S(\square), \circ)$ and (U_{12}, \times_{12}) are given below. The elements in the borders are arranged in an order that gives the tables the same pattern, so we know that these two groups are isomorphic.

| \circ | e | a | r | s |
|---------|-----|-----|-----|-----|
| e | e | a | r | s |
| a | a | e | s | r |
| r | r | s | e | a |
| s | s | r | a | e |

$(S(\square), \circ)$

| \times_{12} | 1 | 5 | 7 | 11 |
|---------------|----|----|----|----|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

(U_{12}, \times_{12})

- (a) Find three different isomorphisms from $(S(\square), \circ)$ to (U_{12}, \times_{12}) .
- (b) Find a one-to-one and onto mapping from $(S(\square), \circ)$ to (U_{12}, \times_{12}) that is not an isomorphism.

Exercise E100

The group tables of the groups $(S^+(\square), \circ)$ and (U_{10}, \times_{10}) are given below. Again the elements in the borders are arranged in an order that gives the tables the same pattern, so we know that these two groups are isomorphic. (Recall that $(S^+(\square), \circ)$ is the group of direct symmetries of the square: see Figure 3.)

| \circ | e | a | b | c |
|---------|-----|-----|-----|-----|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

$(S^+(\square), \circ)$

| \times_{10} | 1 | 3 | 9 | 7 |
|---------------|---|---|---|---|
| 1 | 1 | 3 | 9 | 7 |
| 3 | 3 | 9 | 7 | 1 |
| 9 | 9 | 7 | 1 | 3 |
| 7 | 7 | 1 | 3 | 9 |

(U_{10}, \times_{10})

Find a one-to-one and onto mapping from $(S^+(\square), \circ)$ to (U_{10}, \times_{10}) that maps the identity element of $(S^+(\square), \circ)$ to the identity element of (U_{10}, \times_{10}) but is *not* an isomorphism.

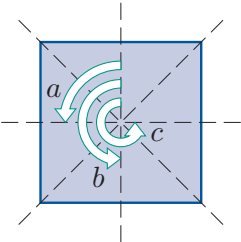


Figure 3 $S^+(\square)$

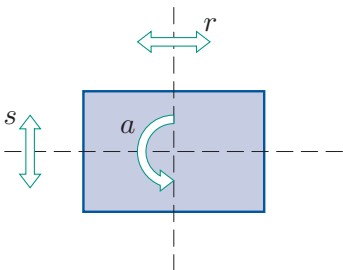


Figure 4 $S(\square)$

It is permissible for the domain group and the codomain group of an isomorphism to be the same group. For example, consider the following mapping.

$$\begin{aligned}\phi : (S(\square), \circ) &\longrightarrow (S(\square), \circ) \\ e &\longmapsto e \\ a &\longmapsto a \\ r &\longmapsto s \\ s &\longmapsto r\end{aligned}$$

(The non-identity symmetries of $S(\square)$ are shown again in Figure 4.)

If we replace each entry in the group table of $(S(\square), \circ)$ shown on the left below with its image under ϕ , then we obtain the table on the right below.

| \circ | e | a | r | s | | e | a | s | r |
|---------|-----|-----|-----|-----|--|-----|-----|-----|-----|
| e | e | a | r | s | | e | e | a | s |
| a | a | e | s | r | | a | a | e | r |
| r | r | s | e | a | | s | s | r | e |
| s | s | r | a | e | | r | r | s | a |

$(S(\square), \circ)$

This second table is a correct group table for $(S(\square), \circ)$, so ϕ is an isomorphism.

An isomorphism from a group to itself is called an **automorphism** of the group. Thus the mapping ϕ above is an automorphism of $(S(\square), \circ)$.

Exercise E101

Find two automorphisms of $(S(\square), \circ)$ other than the one above.

If there are no isomorphisms at all between two groups, then the groups are not isomorphic. This is always the case for two groups of different orders, because there are not even any one-to-one and onto functions between such groups. However, even if two groups have the same order, there may be no isomorphisms between them. For example, consider the groups $(S(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$, whose group tables are given below.

| \circ | e | a | r | s | | $+_4$ | 0 | 1 | 2 | 3 |
|---------|-----|-----|-----|-----|--|-------|---|---|---|---|
| e | e | a | r | s | | 0 | 0 | 1 | 2 | 3 |
| a | a | e | s | r | | 1 | 1 | 2 | 3 | 0 |
| r | r | s | e | a | | 2 | 2 | 3 | 0 | 1 |
| s | s | r | a | e | | 3 | 3 | 0 | 1 | 2 |

$(S(\square), \circ)$ $(\mathbb{Z}_4, +_4)$

It is not possible to find a mapping from $(S(\square), \circ)$ to $(\mathbb{Z}_4, +_4)$ that transforms the group table of $(S(\square), \circ)$ into a group table for $(\mathbb{Z}_4, +_4)$. To see this, notice that in $(S(\square), \circ)$ all the elements are self-inverse, so the identity element appears in each of the four positions on the main diagonal. So every mapping from $S(\square)$ to \mathbb{Z}_4 will transform the group table of $(S(\square), \circ)$ into a table in which all four positions on the main diagonal contain the same element. However, in $(\mathbb{Z}_4, +_4)$ two of the elements (0 and 2) are self-inverse and the other two elements (1 and 3) are inverses of each other, so in any group table for $(\mathbb{Z}_4, +_4)$ two of the positions on the main diagonal will contain the identity element and two will not, no matter how the elements of $(\mathbb{Z}_4, +_4)$ are arranged in the table borders. Thus there is no mapping that transforms the group table of $(S(\square), \circ)$ into a group table for $(\mathbb{Z}_4, +_4)$. That is, there is no isomorphism

from $(S(\square), \circ)$ to $(\mathbb{Z}_4, +_4)$. These two groups have fundamentally different structures: they are not isomorphic.

Matching up group tables can help us investigate isomorphisms between small groups, but it is not feasible for most groups. So we need an algebraic way to express the properties that a mapping ϕ from a group (G, \circ) to a group $(H, *)$ must satisfy in order to be an isomorphism. The definition that we need was given in Subsection 4.2 of Unit B2 and is restated below. It applies to both finite and infinite groups.

Definitions

Let (G, \circ) and $(H, *)$ be groups. A mapping $\phi : (G, \circ) \longrightarrow (H, *)$ is an **isomorphism** if it has the following two properties:

- (a) ϕ is one-to-one and onto
- (b) $\phi(x \circ y) = \phi(x) * \phi(y)$ for all $x, y \in G$.

If an isomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ exists, then (G, \circ) and $(H, *)$ are **isomorphic**. Otherwise they are **non-isomorphic**.

We write $(G, \circ) \cong (H, *)$ (or simply $G \cong H$ when the operations \circ and $*$ are clear) to assert that the groups (G, \circ) and $(H, *)$ are isomorphic.

Property (a) in the definition ensures that ϕ is a one-to-one correspondence between the two groups; that is, it matches up each element of (G, \circ) with exactly one element of $(H, *)$ and vice versa. Property (b) ensures that the way that elements combine in (G, \circ) matches up with the way that their corresponding elements combine in $(H, *)$. To see why it is needed, suppose that the group (G, \circ) is finite, so we can construct its group table, and consider its elements x and y and their composite $x \circ y$ in the group table of (G, \circ) , as illustrated on the left below. In the table transformed by using a mapping $\phi : (G, \circ) \longrightarrow (H, *)$, these three elements are replaced by $\phi(x)$, $\phi(y)$ and $\phi(x \circ y)$, as illustrated on the right.

| \circ | \cdots | y | \cdots | | $*$ | \cdots | $\phi(y)$ | \cdots |
|--------------|----------|-------------|----------|-------------------|-----------|----------|-------------------|----------|
| \vdots | | \vdots | | | \vdots | | \vdots | |
| x | \cdots | $x \circ y$ | \cdots | \longrightarrow | $\phi(x)$ | \cdots | $\phi(x \circ y)$ | \cdots |
| \vdots | | \vdots | | | \vdots | | \vdots | |
| (G, \circ) | | | | | $(H, *)$ | | | |

If the table on the right is to be a correct group table for $(H, *)$, then the entry in the cell with row label $\phi(x)$ and column label $\phi(y)$ must be equal to $\phi(x) * \phi(y)$, so we must have

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

This equation must hold for all elements x and y of G , which gives property (b). The property is needed for essentially the same reasons when G is infinite – the only difference is that we cannot construct a complete group table for an infinite group (G, \circ) .

A mapping ϕ from one group to another that satisfies property (b) is said to **preserve composites**. This property means that for any two elements from the domain group G , we can do *either* of the following and we will obtain the same answer either way.

- First compose the two elements in the domain group G using \circ , then map their composite using ϕ . (That is, find $\phi(x \circ y)$.)
- First map each of the two elements individually using ϕ , then compose the resulting images in the codomain group H using $*$. (That is, find $\phi(x) * \phi(y)$.)

This is illustrated in Figure 5.

Here is a worked exercise that demonstrates how to show that a mapping from one group to another is an isomorphism.

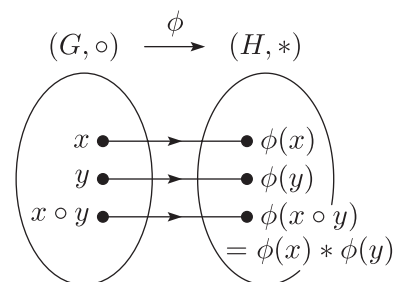


Figure 5 Preserving composites

Worked Exercise E37

Prove that the following mapping ϕ is an isomorphism:

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (2\mathbb{Z}, +) \\ n &\longmapsto 2n.\end{aligned}$$

(Recall that $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$. We know that $(2\mathbb{Z}, +)$ is a group because it is the cyclic subgroup of the group $(\mathbb{Z}, +)$ generated by the element 2.)

Solution

First we show that ϕ is one-to-one and onto.

To show that ϕ is one-to-one, suppose that m and n are elements of \mathbb{Z} such that

$$\phi(m) = \phi(n).$$

Then

$$2m = 2n,$$

which gives

$$m = n.$$

Thus ϕ is one-to-one.

Also, ϕ is onto, because any element of $2\mathbb{Z}$ is of the form $2n$ where $n \in \mathbb{Z}$, and this element is the image under ϕ of the element n of \mathbb{Z} .

Now we show that ϕ preserves composites. It is helpful to start by taking two general elements of the domain group and writing down the equation that we have to prove in terms of these elements. This is obtained from the equation

$$\phi(x \circ y) = \phi(x) * \phi(y)$$

in the definition of an isomorphism by replacing:

- x and y by general elements of the domain group,
- \circ by the binary operation of the domain group,
- $*$ by the binary operation of the codomain group.

To check that ϕ preserves composites, let m and n be elements of \mathbb{Z} . We have to show that

$$\phi(m + n) = \phi(m) + \phi(n).$$

Now

$$\begin{aligned}\phi(m + n) &= 2(m + n) \\ &= 2m + 2n \\ &= \phi(m) + \phi(n).\end{aligned}$$

Thus ϕ preserves composites.

Hence ϕ is an isomorphism.

The next worked exercise provides another example of how to show that a mapping from one group to another is an isomorphism. It involves an interesting mapping: the natural logarithm function, \log . The properties of this function used in the worked exercise were given in Subsection 4.2 of Unit D4 *Continuity*.

Worked Exercise E38

Show that the following mapping is an isomorphism:



$$\begin{aligned}\phi : (\mathbb{R}^+, \times) &\longrightarrow (\mathbb{R}, +) \\ x &\longmapsto \log x.\end{aligned}$$

Solution

We check that ϕ is one-to-one and onto.

The mapping ϕ (the natural logarithm function) is one-to-one.

It is also onto, because its image set is \mathbb{R} , which is its codomain.

 We now check that ϕ preserves composites. As in Worked Exercise E37, we start by taking two general elements of the domain group, and write down the equation that has to be proved. Here the binary operations of the domain group and codomain group are \times and $+$, respectively. 

To check that ϕ preserves composites, let $x, y \in \mathbb{R}^+$. We have to show that

$$\phi(x \times y) = \phi(x) + \phi(y),$$

that is,

$$\log(x \times y) = \log x + \log y.$$

This is true by the properties of the function \log , so ϕ preserves composites.

Hence ϕ is an isomorphism.

Worked Exercise E38 shows that the two groups (\mathbb{R}^+, \times) and $(\mathbb{R}, +)$ are isomorphic.

The isomorphism in Worked Exercise E38 was widely used when doing complicated arithmetic before the days of calculators. It was easier to multiply long numbers by adding logarithms than by performing long multiplication. This was called ‘using logs’.

Exercise E102

Show that the mapping

$$\begin{aligned} \phi : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto e^x \end{aligned}$$

is an isomorphism. You can use any of the properties of the exponential function given in Subsections 4.2 and 4.3 of Unit D4.

The isomorphism in Exercise E102 is the inverse function of the isomorphism in Worked Exercise E38. The inverse function of an isomorphism is always an isomorphism, as discussed later in this subsection.

In the next exercise you are asked to show that a particular mapping from a group to itself is an isomorphism. In other words, you are asked to show that this mapping is an automorphism of the group.

Exercise E103

Show that the following mapping is an isomorphism:

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto -n.\end{aligned}$$

The next worked exercise demonstrates how to show that a mapping from a group to a group is *not* an isomorphism.

Worked Exercise E39

Explain why each of the following mappings is not an isomorphism.

$$\begin{array}{ll} \text{(a)} \quad \phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}, +) & \text{(b)} \quad \phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^+, \times) \\ n \longmapsto 2n & x \longmapsto |x| \end{array}$$

$$\begin{array}{l} \text{(c)} \quad \phi : (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_5^*, \times_5) \\ 0 \longmapsto 1 \\ 1 \longmapsto 4 \\ 2 \longmapsto 3 \\ 3 \longmapsto 2 \end{array}$$

Solution

- (a) This mapping ϕ is not onto: for example, the element π of the codomain \mathbb{R} is not the image of any element in the domain \mathbb{Z} .
- (b) This mapping ϕ is not one-to-one: for example, $\phi(2) = \phi(-2) = 2$.
- (c) This mapping ϕ does not preserve composites. To preserve composites it must have the property that for all $m, n \in \mathbb{Z}_4$,

$$\phi(m +_4 n) = \phi(m) \times_5 \phi(n).$$

However, $1, 3 \in \mathbb{Z}_4$ and

$$\phi(1 +_4 3) = \phi(0) = 1,$$

whereas

$$\phi(1) \times_5 \phi(3) = 4 \times_5 2 = 3,$$

so

$$\phi(1 +_4 3) \neq \phi(1) \times_5 \phi(3).$$

Exercise E104

The following mappings are not isomorphisms. In each case, show that one of the conditions in the definition of an isomorphism fails to hold.

- (a) $\phi : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{R}^+, \times)$ (b) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
 $z \longmapsto |z|$ $n \longmapsto 5n$
- (c) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$
 $x \longmapsto 2^x$

In Worked Exercise E38 and Exercise E102 earlier in this subsection you saw that the mapping

$$\begin{aligned}\phi : (\mathbb{R}^+, \times) &\longrightarrow (\mathbb{R}, +) \\ x &\longmapsto \log x\end{aligned}$$

and its inverse

$$\begin{aligned}\phi^{-1} : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto e^x\end{aligned}$$

are both isomorphisms. In general, if ϕ is an isomorphism from a group (G, \circ) to a group $(H, *)$, then ϕ^{-1} is an isomorphism from $(H, *)$ to (G, \circ) . This makes sense, because if the mapping ϕ ‘renames’ (G, \circ) to $(H, *)$, then its inverse ϕ^{-1} must rename $(H, *)$ to (G, \circ) . This fact is stated as a proposition below, with a formal proof using the definition of an isomorphism given earlier in this subsection.

Proposition E36

Let (G, \circ) and $(H, *)$ be groups. If ϕ is an isomorphism from (G, \circ) to $(H, *)$, then ϕ^{-1} is an isomorphism from $(H, *)$ to (G, \circ) .

Proof Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism. Since ϕ is one-to-one and onto, its inverse mapping $\phi^{-1} : (H, *) \longrightarrow (G, \circ)$ exists and is also one-to-one and onto. Let h_1 and h_2 be any elements of H . Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. So

$$\begin{aligned}\phi^{-1}(h_1 * h_2) &= \phi^{-1}(\phi(g_1) * \phi(g_2)) \\ &= \phi^{-1}(\phi(g_1 \circ g_2)) \quad (\text{since } \phi \text{ preserves composites}) \\ &= g_1 \circ g_2 \\ &= \phi^{-1}(h_1) \circ \phi^{-1}(h_2).\end{aligned}$$

Hence ϕ^{-1} is an isomorphism, as claimed. ■

Isomorphisms of cyclic groups

You studied isomorphisms of *cyclic* groups in Subsection 4.4 of Unit B2. You met the following theorems.

Theorems B49 and B50

Let (G, \circ) and $(H, *)$ be cyclic groups, generated by a and b , respectively.

- If (G, \circ) and $(H, *)$ have the same finite order n , then they are isomorphic and an isomorphism is given by

$$\begin{aligned}\phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k = 0, 1, \dots, n-1).\end{aligned}$$

- If (G, \circ) and $(H, *)$ both have infinite order, then they are isomorphic and an isomorphism is given by

$$\begin{aligned}\phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k \in \mathbb{Z}).\end{aligned}$$



The next worked exercise illustrates how to use the first of these results to find isomorphisms between two cyclic groups of the same finite order.

Worked Exercise E40



Find two isomorphisms from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

Solution

Both of these groups are cyclic groups of order 4.

 To find an isomorphism between them, we first find a generator of each group. 


The group $(\mathbb{Z}_4, +_4)$ is generated by 1.

 To find a generator of $(\mathbb{Z}_5^*, \times_5)$, we try finding consecutive powers of 2, say, to see whether it generates the whole of \mathbb{Z}_5^* . 

The consecutive powers of 2 in $(\mathbb{Z}_5^*, \times_5)$ starting from 2^0 are:


$$1, 2, 4, 3, \dots$$

All the elements of \mathbb{Z}_5^* appear in this list, so 2 is a generator of $(\mathbb{Z}_5^*, \times_5)$.

 To write down an isomorphism, we match up corresponding multiples/powers of the generators (depending on whether the groups are additive or multiplicative), starting by matching the zeroth



multiples/powers (the identities). This gives:

$$\begin{array}{ll}
 (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_5^*, \times_5) & (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_5^*, \times_5) \\
 0 \mapsto 1 & 0 \mapsto 1 \\
 1 \mapsto 2 & \text{that is, } 1 \mapsto 2 \\
 1 +_4 1 \mapsto 2 \times_5 2 & 2 \mapsto 4 \\
 1 +_4 1 +_4 1 \mapsto 2 \times_5 2 \times_5 2, & 3 \mapsto 3.
 \end{array}$$

For example, here we have matched the second *multiple* of the generator 1 in $(\mathbb{Z}_4, +_4)$, that is, $1 +_4 1$, with the second *power* of the generator 2 in $(\mathbb{Z}_5^*, \times_5)$, that is, $2 \times_5 2$. 

Hence an isomorphism is given by

$$\begin{array}{l}
 \phi_1 : (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_5^*, \times_5) \\
 0 \mapsto 1 \\
 1 \mapsto 2 \\
 2 \mapsto 4 \\
 3 \mapsto 3.
 \end{array}$$

 To find a different isomorphism, we find a different generator of *one* of the groups, and match up powers/multiples of the generators in the same way as above. 

The group $(\mathbb{Z}_5^*, \times_5)$ is also generated by 3 (since 3 is the inverse of 2 in $(\mathbb{Z}_5^*, \times_5)$). The consecutive powers of 3 in $(\mathbb{Z}_5^*, \times_5)$ starting from $3^0 = 1$ are

$$1, 3, 4, 2, \dots$$

So another isomorphism is given by

$$\begin{array}{l}
 \phi_2 : (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_5^*, \times_5) \\
 0 \mapsto 1 \\
 1 \mapsto 3 \\
 2 \mapsto 4 \\
 3 \mapsto 2.
 \end{array}$$

The next two exercises give you practice in finding isomorphisms between finite cyclic groups of the same order.

Exercise E105

Find an isomorphism from the group $(\mathbb{Z}_{10}, +_{10})$ to the group $(\mathbb{Z}_{11}^*, \times_{11})$.

Exercise E106

Find an isomorphism from the group $(\mathbb{Z}_4, +_4)$ to the cyclic subgroup of $(\mathbb{Z}_8, +_8)$ generated by 2.

1.2 Homomorphisms

In the previous subsection you saw that an *isomorphism* is a mapping from one group to another that is one-to-one and onto and also preserves composites.

Now consider the following two mappings from groups to groups: one of them is not one-to-one and the other is not onto (as you saw in Worked Exercise E39(b) and Exercise E104(b), respectively), but they both preserve composites.

- The mapping

$$\begin{aligned}\phi : (\mathbb{R}^*, \times) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto |x|\end{aligned}$$

is not one-to-one but is onto. It preserves composites since for all $x, y \in \mathbb{R}^*$,

$$\phi(x \times y) = |x \times y| = |x| \times |y| = \phi(x) \times \phi(y).$$

- The mapping

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto 5n\end{aligned}$$

is one-to-one but is not onto. It preserves composites since for all $m, n \in \mathbb{Z}$,

$$\phi(m + n) = 5(m + n) = 5m + 5n = \phi(m) + \phi(n).$$

A mapping from a group to a group that preserves composites but is not necessarily one-to-one or onto is called a *homomorphism*.

Definitions

Let (G, \circ) and $(H, *)$ be groups. A mapping $\phi : (G, \circ) \longrightarrow (H, *)$ is a **homomorphism** if it has the property

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G.$$

This property is called the **homomorphism property**.

Thus ‘the homomorphism property’ is just another name for the property of preserving composites.

A homomorphism that is both one-to-one and onto is an isomorphism.

It is important to appreciate that the homomorphism property is not likely to hold for a randomly chosen mapping between two groups. Consider any mapping ϕ from a group (G, \circ) to a group $(H, *)$. In Figure 6, going from left to right *across* the diagram represents mapping from G to H using ϕ , while going *down* the diagram represents combining elements within a group, namely within (G, \circ) on the left and within $(H, *)$ on the right.

Starting with two elements x and y in G , as shown in the top left-hand corner, we can combine them in (G, \circ) to obtain the element $x \circ y$ of G and then map this element using ϕ to obtain the element $\phi(x \circ y)$ of H .

Alternatively we can map the elements x and y individually using ϕ to obtain the elements $\phi(x)$ and $\phi(y)$ of H and then combine these elements in $(H, *)$ to obtain the element $\phi(x) * \phi(y)$ of H . In general there is no reason why there should be any connection between the elements $\phi(x \circ y)$ and $\phi(x) * \phi(y)$ of H , but if they are equal for *every* choice of x and y from G , then the mapping ϕ is a homomorphism.

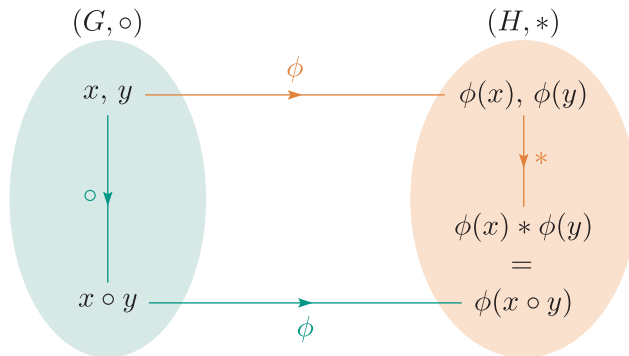


Figure 6 The homomorphism property

The worked exercise below demonstrates how to show that a mapping is a homomorphism. Doing this is just the same as checking property (b) in the definition of an isomorphism.

Worked Exercise E41

Show that the following mapping is a homomorphism:

$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z|.\end{aligned}$$

Solution

To show that ϕ has the homomorphism property, we start by taking two general elements of the domain group and writing down the equation that we have to prove in terms of them, being careful to use the correct binary operation on each side of the equation.

Let $z, w \in \mathbb{C}^*$. We have to show that

$$\phi(z \times w) = \phi(z) \times \phi(w).$$

Now

$$\phi(z \times w) = |z \times w| = |z| \times |w| = \phi(z) \times \phi(w),$$

by a standard property of complex numbers (given in Subsection 2.2 of Unit A2 *Number systems*). Hence ϕ is a homomorphism.

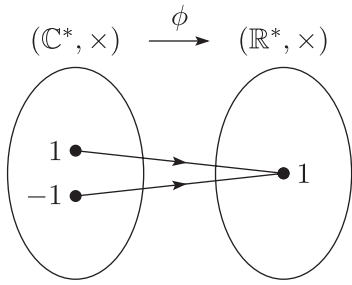


Figure 7 The homomorphism ϕ in Worked Exercise E41 is not one-to-one

Notice that the homomorphism

$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z|\end{aligned}$$

in Worked Exercise E41 is not an isomorphism. It is not one-to-one because, for example, the elements 1 and -1 of the domain group are both mapped by ϕ to the element 1 of the codomain group, as illustrated in Figure 7. It is not onto either, because, for example, the element -1 of the codomain group is not the image of any element of the domain group.

To show that a mapping ϕ from a group (G, \circ) to a group $(H, *)$ is *not* a homomorphism, we have to find a counterexample that demonstrates that the homomorphism property does not hold for ϕ . That is, we have to find two elements $x, y \in G$ for which

$$\phi(x \circ y) \neq \phi(x) * \phi(y).$$

This is demonstrated in the next worked exercise.

Worked Exercise E42

Show that the following mapping is not a homomorphism:

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto 2n + 3.\end{aligned}$$

Solution

The homomorphism property for ϕ is

$$\phi(m + n) = \phi(m) + \phi(n) \quad \text{for all } m, n \in \mathbb{Z}.$$

Now $1, 2 \in \mathbb{Z}$, and

$$\phi(1 + 2) = \phi(3) = 9,$$

but

$$\phi(1) + \phi(2) = 5 + 7 = 12.$$

Thus $\phi(1 + 2) \neq \phi(1) + \phi(2)$, so ϕ is not a homomorphism.

The next exercise asks you to determine whether several mappings are homomorphisms. In each part, start by writing down the homomorphism property for the mapping, try to guess whether it holds, and proceed with a proof or counterexample as appropriate. If you find it difficult to guess, then try checking the homomorphism property: if you find that you cannot complete the check, you may have gained some insight that will help you find a counterexample. When looking for a counterexample, try something simple first – remember that you need only *one* counterexample to show that a mapping is not a homomorphism.

Another useful tip is that when you are trying to check the homomorphism property equation $\phi(x \circ y) = \phi(x) * \phi(y)$, there are various ways to approach it: you can

- start with the left-hand side and show that it is equal to the right-hand side
- do the reverse
- simplify each side separately and check that you get the same answers.

The third approach is often useful in complicated cases.

Exercise E107

Determine which of the following mappings are homomorphisms.

- (a) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$ (b) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
 $x \longmapsto x^2$ $n \longmapsto n^2$
- (c) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$ (d) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, \times)$
 $n \longmapsto 3 \times_6 n$ $n \longmapsto 2^n$
- (e) $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{Z}_2, +_2)$
 $x \longmapsto \begin{cases} 0 & \text{if } x \text{ is rational,} \\ 1 & \text{if } x \text{ is irrational.} \end{cases}$
- (f) $\phi : (\mathbb{R}^2, +) \longrightarrow (\mathbb{R}^2, +)$
 $(x, y) \longmapsto (2x - y, 6x - 3y)$

In the next worked exercise a mapping is shown to be a homomorphism by separately considering several possibilities for the natures of the elements of the domain group.

Worked Exercise E43

Let F be any figure. Show that the mapping

$$\phi : (S(F), \circ) \longrightarrow (\{1, -1\}, \times)$$

$$f \longmapsto \begin{cases} 1 & \text{if } f \text{ is a direct symmetry} \\ -1 & \text{if } f \text{ is an indirect symmetry} \end{cases}$$

is a homomorphism.

(Remember that $S(F)$ denotes the symmetry group of the figure F .

You saw that $(\{1, -1\}, \times)$ is a group in Exercise B21(f) in Subsection 3.3 of Unit B1 *Symmetry and groups*.)

Solution

Let $f, g \in S(F)$. We have to show that

$$\phi(f \circ g) = \phi(f) \times \phi(g).$$

We know that a composite of two direct symmetries or two indirect symmetries is direct, and a composite of a direct symmetry and an indirect symmetry is indirect. Thus we have the following.

If f is direct and g is direct then $f \circ g$ is direct so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) \times \phi(g) = 1 \times 1 = 1.$$

If f is direct and g is indirect then $f \circ g$ is indirect so

$$\phi(f \circ g) = -1 \quad \text{and} \quad \phi(f) \times \phi(g) = 1 \times (-1) = -1.$$

If f is indirect and g is direct then $f \circ g$ is indirect so

$$\phi(f \circ g) = -1 \quad \text{and} \quad \phi(f) \times \phi(g) = (-1) \times 1 = -1.$$

If f is indirect and g is indirect then $f \circ g$ is direct so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) \times \phi(g) = (-1) \times (-1) = 1.$$

Thus in all cases $\phi(f \circ g) = \phi(f) \times \phi(g)$. Hence ϕ is a homomorphism.

Exercise E108

Let n be an integer greater than 1. Show that the mapping

$$\begin{aligned} \phi : (S_n, \circ) &\longrightarrow (\mathbb{Z}_2, +_2) \\ f &\longmapsto \begin{cases} 0 & \text{if } f \text{ is an even permutation} \\ 1 & \text{if } f \text{ is an odd permutation} \end{cases} \end{aligned}$$

is a homomorphism.

(Remember that S_n is the symmetric group of degree n , that is, the group of all permutations of $\{1, 2, \dots, n\}$.)

We will now look at some homomorphisms whose domain groups, and in some cases also codomain groups, are matrix groups.

Recall that the group of invertible 2×2 matrices with real entries under matrix multiplication is denoted by $\text{GL}(2)$:

$$\text{GL}(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}.$$

Remember also that throughout this book we use L to denote the group of invertible 2×2 lower triangular matrices with real entries, and D to denote the group of invertible 2×2 diagonal matrices with real entries,

each under matrix multiplication:

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0 \right\},$$

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\}.$$

Worked Exercise E44

Show that the following mapping is a homomorphism:

$$\begin{aligned} \phi : (L, \times) &\longrightarrow (L, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix}. \end{aligned}$$

Solution

Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{A} \times \mathbf{B}) = \phi(\mathbf{A}) \times \phi(\mathbf{B});$$

that is,

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$.

Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi \left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \right) \\ &= \phi \begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & (uy)^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & u^2y^2 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \phi \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & u^2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & y^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & u^2y^2 \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

Note that for simplicity we write $\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $\phi \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)$.

This convention is used in the solution to Worked Exercise E44 above.

Exercise E109

Show that the following mappings are homomorphisms.

$$\begin{aligned} \text{(a)} \quad \phi : (L, \times) &\longrightarrow (D, \times) & \text{(b)} \quad \phi : (L, \times) &\longrightarrow (L, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} & \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} a & 0 \\ a-d & d \end{pmatrix} \end{aligned}$$

Exercise E110

Show that the following mapping is not a homomorphism:

$$\begin{aligned} \phi : (\text{GL}(2), \times) &\longrightarrow (\text{GL}(2), \times) \\ \mathbf{A} &\longmapsto \mathbf{A}^{-1}. \end{aligned}$$

Exercise E111

Determine whether each of the following mappings is a homomorphism, justifying your answers.

$$\begin{aligned} \text{(a)} \quad \phi : (L, \times) &\longrightarrow (\mathbb{R}, +) & \text{(b)} \quad \phi : (L, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto a + d & \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto a^2 d^2 \\ \text{(c)} \quad \phi : (L, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \frac{a}{d} \end{aligned}$$

The proposition below provides some nice examples of homomorphisms that map from an infinite group to a finite group. Here, and throughout this unit, the notation $k_{(\text{mod } n)}$, where k is any integer and n is any integer with $n \geq 2$, is used to denote the **least residue of k modulo n** , which is the integer in \mathbb{Z}_n that is congruent to k modulo n . In other words, $k_{(\text{mod } n)}$ is the remainder of k on division by n . For example,

$$8_{(\text{mod } 5)} = 3, \quad 5_{(\text{mod } 5)} = 0 \quad \text{and} \quad -1_{(\text{mod } 5)} = 4.$$

Proposition E37

For any integer $n \geq 2$, the following mapping is a homomorphism:

$$\begin{aligned} \phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}_n, +_n) \\ k &\longmapsto k_{(\text{mod } n)}. \end{aligned}$$

Proof Let n be an integer with $n \geq 2$, and let ϕ be the mapping defined above. Let $r, s \in \mathbb{Z}$. We have to show that

$$\phi(r + s) = \phi(r) +_n \phi(s),$$

that is,

$$(r + s)_{(\text{mod } n)} = r_{(\text{mod } n)} +_n s_{(\text{mod } n)}.$$

Now, modulo n we have

$$\begin{aligned} r_{(\text{mod } n)} +_n s_{(\text{mod } n)} &\equiv r_{(\text{mod } n)} + s_{(\text{mod } n)} \quad (\text{by the definition of } +_n) \\ &\equiv r + s \quad (\text{since } r_{(\text{mod } n)} \equiv r \text{ and } s_{(\text{mod } n)} \equiv s) \\ &\equiv (r + s)_{(\text{mod } n)} \quad (\text{by the definition of least residue}). \end{aligned}$$

But both $r_{(\text{mod } n)} +_n s_{(\text{mod } n)}$ and $(r + s)_{(\text{mod } n)}$ are elements of \mathbb{Z}_n , so they must be equal, as required. ■

For example, the homomorphism given by Proposition E37 for $n = 3$ is as follows.

$$\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_3, +_3)$$

$$\begin{array}{l} \vdots \\ -2 \longmapsto 1 \\ -1 \longmapsto 2 \\ 0 \longmapsto 0 \\ 1 \longmapsto 1 \\ 2 \longmapsto 2 \\ 3 \longmapsto 0 \\ 4 \longmapsto 1 \\ \vdots \end{array}$$

In the next exercise you are asked to prove a result involving homomorphisms.

Exercise E112

Prove that the mapping

$$\begin{aligned} \phi : (G, \circ) &\longrightarrow (G, \circ) \\ x &\longmapsto x \circ x \end{aligned}$$

is a homomorphism if and only if G is abelian.

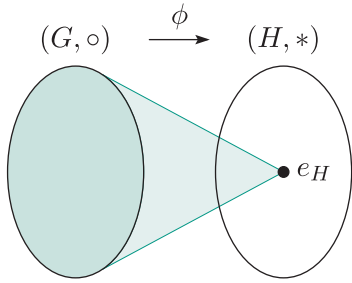


Figure 8 The trivial homomorphism from (G, \circ) to $(H, *)$

The trivial homomorphism

Given any two groups (G, \circ) and $(H, *)$, there is always at least one homomorphism from (G, \circ) to $(H, *)$, namely the mapping that maps every element of (G, \circ) to the identity element of $(H, *)$, as illustrated in Figure 8. A proof that this mapping is a homomorphism is given below. It is called the **trivial homomorphism** from (G, \circ) to $(H, *)$.

Proposition E38

Let (G, \circ) and $(H, *)$ be groups, and let the identity element of $(H, *)$ be e_H . Then the following mapping is a homomorphism:

$$\begin{aligned}\phi : (G, \circ) &\longrightarrow (H, *) \\ x &\longmapsto e_H.\end{aligned}$$

Proof Let $x, y \in G$. Then, since ϕ maps every element of G to e_H , we have

$$\phi(x \circ y) = e_H$$

and

$$\phi(x) * \phi(y) = e_H * e_H = e_H.$$

Thus $\phi(x \circ y) = \phi(x) * \phi(y)$. Hence ϕ is a homomorphism. ■

Linear transformations as homomorphisms

In Unit C3 you met the idea of a *linear transformation* of a vector space, as follows.

Definition

Let V and W be vector spaces. A function $t : V \longrightarrow W$ is a **linear transformation** if it satisfies the following properties.

LT1 $t(\mathbf{v}_1 + \mathbf{v}_2) = t(\mathbf{v}_1) + t(\mathbf{v}_2), \quad \text{for all } \mathbf{v}_1, \mathbf{v}_2 \in V.$

LT2 $t(\alpha \mathbf{v}) = \alpha t(\mathbf{v}), \quad \text{for all } \mathbf{v} \in V, \alpha \in \mathbb{R}.$

Remember that any vector space is, in particular, a group under vector addition. So a linear transformation maps from a group to a group. It is always a homomorphism between these groups, as shown below.

Proposition E39

Let V and W be vector spaces and let $t : V \longrightarrow W$ be a linear transformation. Then t is a homomorphism from the group $(V, +)$ to the group $(W, +)$.

Proof The homomorphism property for t is

$$t(\mathbf{v}_1 + \mathbf{v}_2) = t(\mathbf{v}_1) + t(\mathbf{v}_2), \quad \text{for all } \mathbf{v}_1, \mathbf{v}_2 \in V.$$

This is the first of the two properties that t must have to be a linear transformation. Hence t is a homomorphism. ■

Thus a linear transformation is a special type of homomorphism: one whose domain group and codomain group are additive groups that are also vector spaces under some type of scalar multiplication, and that satisfies not just the homomorphism property but also a further property involving scalar multiplication (the property is that it ‘preserves scalar multiples’).

We can use Proposition E39 to recognise immediately that some mappings are homomorphisms. For example, consider the mapping

$$\begin{aligned} \phi : (\mathbb{R}^2, +) &\longrightarrow (\mathbb{R}^2, +) \\ (x, y) &\longmapsto (2x - y, 6x - 3y). \end{aligned}$$

You were asked to determine whether this mapping is a homomorphism in Exercise E107(f). Notice that it is a linear transformation from the vector space \mathbb{R}^2 to the vector space \mathbb{R}^2 , because it is of the form

$$(x, y) \longmapsto (ax + by, cx + dy)$$

where $a, b, c, d \in \mathbb{R}$ and hence it has a matrix representation (see Theorem C41 in Unit C3). So it follows immediately from Proposition E39 that it is a homomorphism from the group $(\mathbb{R}^2, +)$ to the group $(\mathbb{R}^2, +)$. There is no need to check the homomorphism property directly, as was done in the solution to Exercise E107(f).

1.3 Properties of homomorphisms

You have seen that an isomorphism, that is, a one-to-one and onto homomorphism, preserves all the structure of its domain group. In contrast, a trivial homomorphism, which maps each element of its domain group to the identity element of its codomain group, preserves very little of the structure. These are two extremes: in general, a homomorphism preserves some, but not necessarily all, of the structure of its domain group, as you will see in this subsection.

We will start by looking at various features of a group that are preserved by homomorphisms.

Preservation of composites of two or more elements

The homomorphism property for a mapping $\phi : (G, \circ) \longrightarrow (H, *)$ is

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G.$$

It is illustrated in Figure 9. This property tells us that a homomorphism preserves composites of *two* elements.

In the next exercise you are asked to prove that a homomorphism also preserves composites of *three* elements.

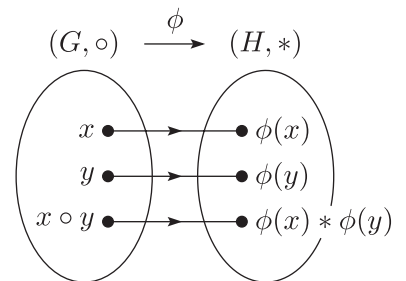


Figure 9 A homomorphism preserves composites

Exercise E113

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Prove that

$$\phi(x \circ y \circ z) = \phi(x) * \phi(y) * \phi(z) \quad \text{for all } x, y, z \in G.$$

Hint: Write $x \circ y \circ z$ as $(x \circ y) \circ z$.

We can use induction to prove that a homomorphism preserves composites of any finite number of elements, as follows.

Proposition E40

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. If x_1, x_2, \dots, x_n are any elements of G , then

$$\phi(x_1 \circ x_2 \circ \dots \circ x_n) = \phi(x_1) * \phi(x_2) * \dots * \phi(x_n).$$

Proof We use induction on the number n of elements. Let $P(n)$ be the statement

$$\phi(x_1 \circ x_2 \circ \dots \circ x_n) = \phi(x_1) * \phi(x_2) * \dots * \phi(x_n) \quad \text{for all } x_1, x_2, \dots, x_n \in G.$$

Then $P(1)$ is

$$\phi(x_1) = \phi(x_1) \quad \text{for all } x_1 \in G.$$

This is true.

Now suppose that $k \in \mathbb{N}$ and $P(k)$ holds; that is

$$\phi(x_1 \circ x_2 \circ \dots \circ x_k) = \phi(x_1) * \phi(x_2) * \dots * \phi(x_k) \quad \text{for all } x_1, x_2, \dots, x_k \in G.$$

We prove that it follows that $P(k+1)$ holds; that is

$$\phi(x_1 \circ x_2 \circ \dots \circ x_{k+1}) = \phi(x_1) * \phi(x_2) * \dots * \phi(x_{k+1}) \quad \text{for all } x_1, x_2, \dots, x_{k+1} \in G.$$

Let $x_1, x_2, \dots, x_{k+1} \in G$. Then

$$\begin{aligned} & \phi(x_1 \circ x_2 \circ \dots \circ x_k \circ x_{k+1}) \\ &= \phi((x_1 \circ x_2 \circ \dots \circ x_k) \circ x_{k+1}) \\ &= \phi(x_1 \circ x_2 \circ \dots \circ x_k) * \phi(x_{k+1}) \\ & \quad \text{(by the homomorphism property for } \phi) \\ &= (\phi(x_1) * \phi(x_2) * \dots * \phi(x_k)) * \phi(x_{k+1}) \quad \text{(since } P(k) \text{ holds)} \\ &= \phi(x_1) * \phi(x_2) * \dots * \phi(x_k) * \phi(x_{k+1}). \end{aligned}$$

That is, $P(k+1)$ holds.

Hence, by the Principle of Mathematical Induction, the statement $P(n)$ is true for every natural number n , which proves the proposition. ■

Proposition E40 is illustrated in Figure 10.

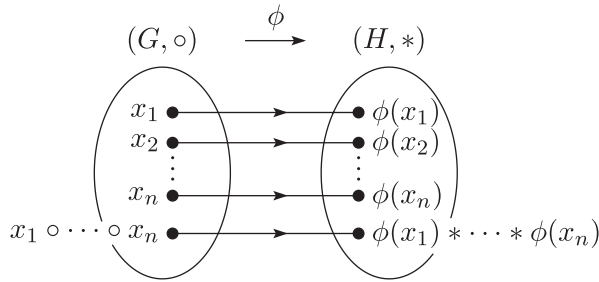


Figure 10 A homomorphism preserves composites of any finite number of elements

Preservation of the identity

You saw in Subsection 4.3 of Unit B2 that any isomorphism maps the identity element of the domain group to the identity element of the codomain group. This is true of homomorphisms in general, as illustrated in Figure 11 and proved below. We say that a homomorphism **preserves the identity**.

Throughout this unit, in discussions about an abstract homomorphism $\phi : (G, \circ) \rightarrow (H, *)$, we will denote the identity elements of the domain group (G, \circ) and codomain group $(H, *)$ by e_G and e_H , respectively, without mentioning this every time.

Proposition E41

Let $\phi : (G, \circ) \rightarrow (H, *)$ be a homomorphism. Then

$$\phi(e_G) = e_H.$$

Proof We have

$$e_G \circ e_G = e_G.$$

Applying the homomorphism ϕ gives

$$\phi(e_G \circ e_G) = \phi(e_G).$$

Since ϕ has the homomorphism property, this gives

$$\phi(e_G) * \phi(e_G) = \phi(e_G),$$

and hence

$$\phi(e_G) * \phi(e_G) = \phi(e_G) * e_H.$$

Applying the Left Cancellation Law now gives

$$\phi(e_G) = e_H,$$

as claimed. ■

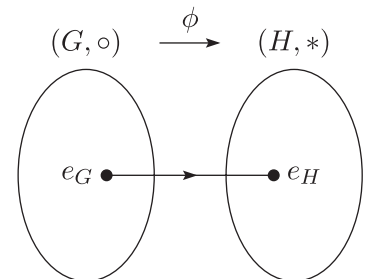


Figure 11 A homomorphism preserves the identity

In the next exercise you are asked to check the property in Proposition E41 for two of the homomorphisms that you met in the previous subsection.

Exercise E114

For each of the following homomorphisms ϕ , state the identity element in the domain group and the identity element in the codomain group, and check that ϕ maps one to the other.

$$(a) \quad \phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times) \quad (b) \quad \phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$$

$$x \longmapsto x^2 \quad n \longmapsto 3 \times_6 n$$

(You saw that these mappings are homomorphisms in Exercise E107.)

Preservation of inverses

You saw in Subsection 4.3 of Unit B2 that an isomorphism maps elements that are inverses of each other in the domain group to elements that are inverses of each other in the codomain group. In other words, for any element x in the domain group,

the image of the inverse of x is the inverse of the image of x .

Again, this is true of homomorphisms in general, as illustrated in Figure 12 and proved below. We say that a homomorphism **preserves inverses**.

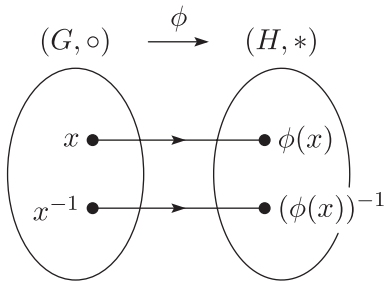


Figure 12 A homomorphism preserves inverses

Proposition E42

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then, for all $x \in G$,

$$\phi(x^{-1}) = (\phi(x))^{-1}.$$

Proof Let $x \in G$. Then

$$x \circ x^{-1} = e_G = x^{-1} \circ x.$$

Applying the homomorphism ϕ gives

$$\phi(x \circ x^{-1}) = \phi(e_G) = \phi(x^{-1} \circ x).$$

Since ϕ has the homomorphism property and since $\phi(e_G) = e_H$ by Proposition E41, this gives

$$\phi(x) * \phi(x^{-1}) = e_H = \phi(x^{-1}) * \phi(x).$$

This shows that $\phi(x^{-1})$ is the inverse of $\phi(x)$ in H ; that is,

$$\phi(x^{-1}) = (\phi(x))^{-1},$$

as claimed. ■

Exercise E115

For each of the following homomorphisms ϕ and elements of their domain groups, state the inverse of the element, find the images under ϕ of the element and its inverse, and verify that these images are the inverses of each other in the codomain group.

- (a) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$ (b) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$
 $x \longmapsto x^2,$ $n \longmapsto 3 \times_6 n,$
 with the element 3 of $(\mathbb{R}^*, \times).$ with the element 4 of $(\mathbb{Z}_6, +_6).$

(These are the same homomorphisms as in Exercise E114.)

Preservation of powers

You saw in Subsection 4.3 of Unit B2 that an isomorphism maps the powers of an element in the domain group to the corresponding powers of the image of the element in the codomain group. In other words, for any element x in the domain group and any integer n ,

the image of the n th power of x is the n th power of the image of x .

Once again this is true of homomorphisms in general, as illustrated in Figure 13 and proved below. We say that a homomorphism **preserves powers**.

Proposition E43

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then, for all $x \in G$ and all $n \in \mathbb{Z}$,

$$\phi(x^n) = (\phi(x))^n.$$

Proof First we use mathematical induction to prove the result for all non-negative integers $n \geq 0$. Then we use Proposition E42 to deduce the result for negative integers.

Case 1: $n \geq 0$

Let $x \in G$ and let $P(n)$ be the statement

$$\phi(x^n) = (\phi(x))^n.$$

Then $P(0)$ is

$$\phi(x^0) = (\phi(x))^0.$$

The zeroth power of any group element is equal to the identity element of the group, so $P(0)$ is just

$$\phi(e_G) = e_H,$$

which is true, by Proposition E41.

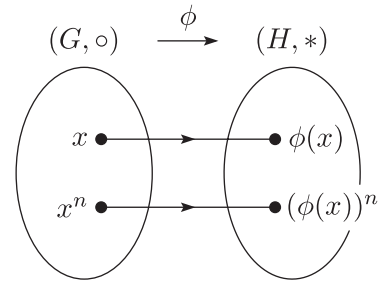


Figure 13 A homomorphism preserves powers

Now let $k \geq 0$ and assume that $P(k)$ is true; that is

$$\phi(x^k) = (\phi(x))^k.$$

We have to deduce that $P(k+1)$ is true; that is,

$$\phi(x^{k+1}) = (\phi(x))^{k+1}.$$

Now

$$\begin{aligned}\phi(x^{k+1}) &= \phi(x^k \circ x) \\ &= \phi(x^k) * \phi(x) \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= (\phi(x))^k * \phi(x) \quad (\text{by } P(k)) \\ &= (\phi(x))^{k+1}.\end{aligned}$$

Thus

$$P(k) \implies P(k+1), \quad \text{for } k = 0, 1, \dots$$

Hence, by mathematical induction, $P(n)$ is true for all $n \geq 0$. This proves the result for $n \geq 0$.

Case 2: $n < 0$

Let $x \in G$ and let $n = -m$, where $m > 0$. Then

$$\begin{aligned}\phi(x^n) &= \phi(x^{-m}) \\ &= \phi((x^{-1})^m) \quad (\text{by the definition of a negative power}) \\ &= (\phi(x^{-1}))^m \quad (\text{by case 1 above, since } m > 0) \\ &= ((\phi(x))^{-1})^m \quad (\text{by Proposition E42}) \\ &= (\phi(x))^{-m} \quad (\text{by the definition of a negative power}) \\ &= (\phi(x))^n,\end{aligned}$$

as required. From cases 1 and 2 it follows that

$$\phi(x^n) = (\phi(x))^n \quad \text{for all } n \in \mathbb{Z}. \quad \blacksquare$$

Notice that Propositions E41 and E42 are special cases of Proposition E43, corresponding to $n = 0$ and $n = -1$, respectively.

Exercise E116

For each of the following homomorphisms ϕ and elements in their domain groups, find $\phi(g^2)$ and $(\phi(g))^2$, where g is the given element, and check that these are equal.

(a) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$

$$x \longmapsto x^2,$$

with the element 3 of (\mathbb{R}^*, \times) .

(b) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$

$$n \longmapsto 3 \times_6 n,$$

with the element 4 of $(\mathbb{Z}_6, +_6)$.

(These are the same homomorphisms as in Exercises E114 and E115.)

Homomorphisms do *not* in general preserve the *orders* of elements. This is apparent from Proposition E38, which states that if (G, \circ) and $(H, *)$ are any groups, then the mapping

$$\begin{aligned}\phi : (G, \circ) &\longrightarrow (H, *) \\ x &\longmapsto e_H\end{aligned}$$

is a homomorphism (the trivial homomorphism).

However, the following theorem holds.

Theorem E44

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism and let x be an element of finite order in G . Then the order of $\phi(x)$ is finite and divides the order of x .

This theorem can be deduced from Proposition E43: a proof is given below. First, here is a lemma that is useful in the proof.

Lemma E45

Let x be an element of a group (G, \circ) . If r is a positive integer such that $x^r = e$, then the order of x divides r .

Proof Suppose that $x^r = e$. Then the order of x is finite; let it be s . By the Division Theorem (Theorem A9 in Unit A2), it follows that there are integers a and b such that $r = as + b$, with $0 \leq b < s$. Now

$$\begin{aligned}e &= x^r \\ &= x^{as+b} \\ &= (x^s)^a \circ x^b \\ &= e^a \circ x^b \quad (\text{since } x \text{ has order } s) \\ &= x^b.\end{aligned}$$

Since s is the *smallest* positive integer such that $x^s = e$, and $0 \leq b < s$, it follows that $b = 0$. Thus $r = as$ and so s divides r . ■

Now here is the proof of Theorem E44.

Proof of Theorem E44 Let the order of x be r . Then

$$\begin{aligned}(\phi(x))^r &= \phi(x^r) \quad (\text{by Proposition E43}) \\ &= \phi(e_G) \quad (\text{since } x \text{ has order } r) \\ &= e_H \quad (\text{by Proposition E41}).\end{aligned}$$

Hence the order of $\phi(x)$ is finite and by Lemma E45 it divides r . ■

Preservation of conjugates

The final result in this subsection concerns the effect of homomorphisms on conjugate elements. We describe this result by saying that homomorphisms **preserve conjugates**.

Proposition E46

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism and let $x, y \in G$.

If x and y are conjugate in (G, \circ) , then $\phi(x)$ and $\phi(y)$ are conjugate in $(H, *)$.

Proof Let x and y be conjugate in (G, \circ) . Then

$$y = g \circ x \circ g^{-1}$$

for some $g \in G$. Hence

$$\begin{aligned}\phi(y) &= \phi(g \circ x \circ g^{-1}) \\ &= \phi(g) * \phi(x) * \phi(g^{-1}) \quad (\text{by Proposition E40}) \\ &= \phi(g) * \phi(x) * (\phi(g))^{-1} \quad (\text{by Proposition E42}).\end{aligned}$$

Since $\phi(g) \in H$, this shows that $\phi(x)$ and $\phi(y)$ are conjugate in $(H, *)$. ■

You have now seen that homomorphisms preserve all of the following:

- composites of any finite number of elements
- the identity
- inverses
- powers
- conjugates.

These properties of homomorphisms will be used to prove some important results later in this unit. They can also help you to recognise whether a mapping is a homomorphism. For example, if a mapping from one group to another does not map the identity of the first group to the identity of the second group, then you know immediately that it is not a homomorphism.

2 Images and kernels

In this section you will learn about two sets associated with a homomorphism: its *image* and its *kernel*. These are essentially the same concepts as the *image set* and *kernel* of a linear transformation, which you met in Section 4 of Unit C3. The *image set* of a function and the *image* of a function are alternative terms for the same concept.

2.1 Image of a homomorphism

You saw in Subsection 3.2 of Unit A1 *Sets, functions and vectors* what is meant by the *image set* of a function: it is the set of all elements in the codomain that are images under the function of elements in the domain. A homomorphism is just a special type of function, so it has an image set, which in group theory we call its *image*. It is defined below and illustrated in Figure 14.

Definition

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. The **image** (or **image set**) of ϕ is

$$\text{Im } \phi = \{\phi(g) : g \in G\}.$$

It is the set of elements of the codomain group H that are images of elements in the domain group G .

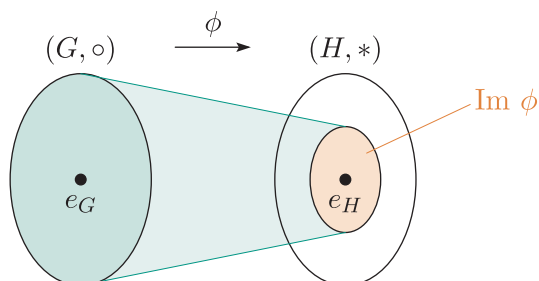


Figure 14 The image of a homomorphism

Remember that in set notation a colon (the symbol ':') means 'such that'. So the notation $\{\phi(g) : g \in G\}$ in the definition above means the set of all $\phi(g)$ such that $g \in G$.

The image of a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ certainly contains e_H , as shown in Figure 14, because $\phi(e_G) = e_H$, by Proposition E41.

The word 'image' has other uses related to functions, of course. In particular, if ϕ is a function (such as a homomorphism) and x is an element of its domain, then $\phi(x)$ is the *image* of x under ϕ . The meaning of any particular instance of the word 'image' should be clear from the context.

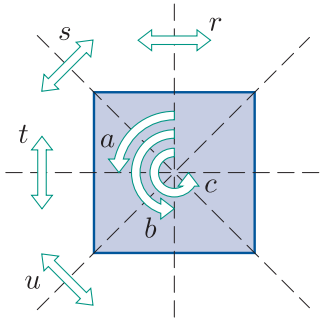


Figure 15 $S(\square)$

Worked Exercise E45

Write down the image of each of the following homomorphisms.

- (a) $\phi_1 : (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_8, +_8)$
- $0 \mapsto 0$
 $1 \mapsto 2$
 $2 \mapsto 4$
 $3 \mapsto 6$
- (b) $\phi_2 : (S(\square), \circ) \longrightarrow (\mathbb{R}^*, \times)$
- $e, a, b, c \mapsto 1$
 $r, s, t, u \mapsto -1$

(The facts that these mappings are homomorphisms follow from Exercise E106 in Subsection 1.1 and Worked Exercise E43 in Subsection 1.2, respectively. The non-identity elements of $S(\square)$ are shown in Figure 15.)

Solution

- (a) The elements of the codomain group \mathbb{Z}_8 that are images under ϕ_1 are 0, 2, 4 and 6.
The image of ϕ_1 is
 $\text{Im } \phi_1 = \{0, 2, 4, 6\}.$
- (b) The elements of the codomain group \mathbb{R}^* that are images under ϕ_2 are -1 and 1 .
The image of ϕ_2 is
 $\text{Im } \phi_2 = \{1, -1\}.$

The images of the homomorphisms in Worked Exercise E45 are illustrated in Figure 16.

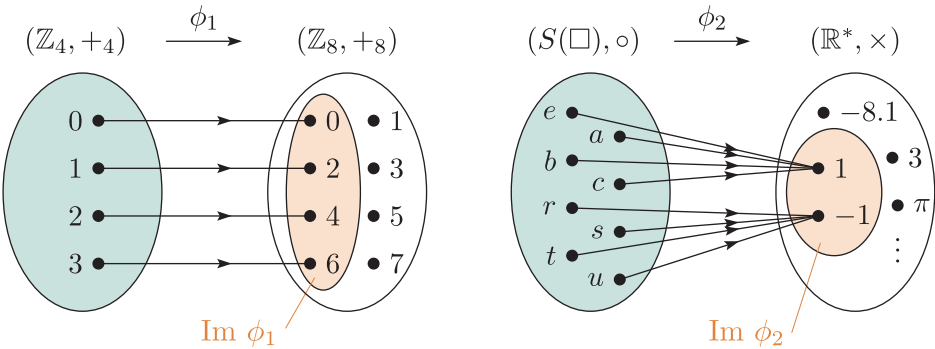


Figure 16 The images of the homomorphisms ϕ_1 and ϕ_2 in Worked Exercise E45

Exercise E117

Write down the image of each of the following homomorphisms.

- (a) $\phi_3 : (S(\square), \circ) \longrightarrow (U_8, \times_8)$ (b) $\phi_4 : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^+, \times)$
- $$\begin{array}{ll} e \longmapsto 1 & x \longmapsto |x| \\ a \longmapsto 3 & \\ r \longmapsto 5 & \\ s \longmapsto 7 & \end{array}$$

(The facts that these mappings are homomorphisms follow from the discussions near the starts of Subsection 1.1 and Subsection 1.2, respectively.)

The mapping ϕ_2 in Figure 16 above illustrates the fact that if $\phi : (G, \circ) \longrightarrow (H, *)$ is a homomorphism, then for each $h \in \text{Im } \phi$ there may be more than one $g \in G$ such that $\phi(g) = h$. In other words, ϕ may not be one-to-one.

As with functions in general, a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ is onto if and only if $\text{Im } \phi = H$. Thus neither of the homomorphisms in Figure 16 is onto. However, both of the homomorphisms in Exercise E117 are onto.

Exercise E118

For each of the following homomorphisms, state whether it is one-to-one and whether it is onto, justifying your answers.

- (a) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_{12}, +_{12})$ (b) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, \times)$
- $$\begin{array}{ll} k \longmapsto k_{(\text{mod } 12)} & n \longmapsto 2^n \end{array}$$

(These mappings are homomorphisms by Proposition E37 and the solution to Exercise E107(d), respectively.)

We now look at an important property of the image of a homomorphism. The image of a homomorphism is, by definition, a subset of the codomain group of the homomorphism. It turns out that it is in fact always a *subgroup* of the codomain group.

To illustrate this, consider again the homomorphisms ϕ_1 , ϕ_2 , ϕ_3 and ϕ_4 from Worked Exercise E45 and Exercise E117. Their codomain groups and images are listed in Table 1 below.

Table 1 Codomain groups and images of four homomorphisms

| Homomorphism | Codomain group | Image |
|--------------|--------------------------|------------------|
| ϕ_1 | $(\mathbb{Z}_8, +_8)$ | $\{0, 2, 4, 6\}$ |
| ϕ_2 | (\mathbb{R}^*, \times) | $\{1, -1\}$ |
| ϕ_3 | (U_8, \times_8) | U_8 |
| ϕ_4 | (\mathbb{R}^+, \times) | \mathbb{R}^+ |

The image of the homomorphism ϕ_1 is the cyclic subgroup of the codomain group generated by the element 2. Similarly, the image of the homomorphism ϕ_2 is the cyclic subgroup of the codomain group generated by the element -1 . The image of the homomorphism ϕ_3 is the whole codomain group, and the same is true for the homomorphism ϕ_4 . So in all four cases the image is a subgroup of the codomain group.

Here is a formal statement and proof of this property.

Theorem E47

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then $\text{Im } \phi$ is a subgroup of $(H, *)$.

Proof We check that the three subgroup properties hold.

SG1 Closure

Let h_1 and h_2 be any elements of $\text{Im } \phi$. Then there are elements $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. We have to show that $h_1 * h_2 \in \text{Im } \phi$. Now

$$\begin{aligned} h_1 * h_2 &= \phi(g_1) * \phi(g_2) \\ &= \phi(g_1 \circ g_2) \quad (\text{since } \phi \text{ is a homomorphism}). \end{aligned}$$

Thus $h_1 * h_2$ is the image of $g_1 \circ g_2$ under ϕ , so $h_1 * h_2 \in \text{Im } \phi$.

SG2 Identity

By Proposition E41, we have $\phi(e_G) = e_H$, so $e_H \in \text{Im } \phi$.

SG3 Inverses

Let $h \in \text{Im } \phi$. Then there is an element $g \in G$ such that $\phi(g) = h$. We have to show that $h^{-1} \in \text{Im } \phi$. Now

$$\begin{aligned} h^{-1} &= (\phi(g))^{-1} \\ &= \phi(g^{-1}) \quad (\text{by Proposition E42}). \end{aligned}$$

Thus h^{-1} is the image of g^{-1} under ϕ , so $h^{-1} \in \text{Im } \phi$.

Since the three subgroup properties hold for $\text{Im } \phi$, it is a subgroup of $(H, *)$. ■

Structure-preserving properties of homomorphisms

When we say that a homomorphism preserves at least some of the structure of the domain group, what we mean is that at least some of the structure of the domain group is present in the image of the homomorphism, which is a group, as you have just seen.

To illustrate this, let us look again at the four homomorphisms ϕ_1 , ϕ_2 , ϕ_3 and ϕ_4 from Worked Exercise E45 and Exercise E117.

First consider ϕ_1 , illustrated in Figure 17. This homomorphism has the additional property that it is one-to-one: each element of $\text{Im } \phi$ is the image of *exactly one* element of the domain group.

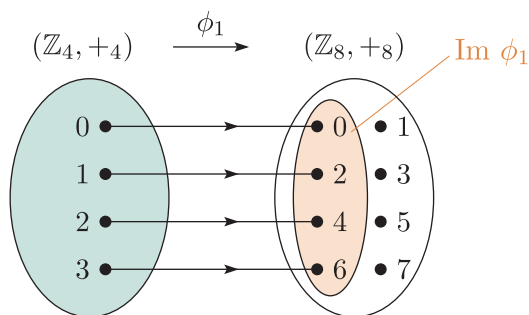


Figure 17 The homomorphism ϕ_1 and its image

It follows that if we ‘shrink’ the codomain of ϕ_1 from $(\mathbb{Z}_8, +_8)$ to its subgroup $\text{Im } \phi = \{0, 2, 4, 6\}$, then ϕ_1 becomes an *isomorphism* from the domain group $(\mathbb{Z}_4, +_4)$ to the image $\text{Im } \phi_1$. Therefore the domain group $(\mathbb{Z}_4, +_4)$ is isomorphic to $\text{Im } \phi_1$. This tells us that ϕ_1 preserves *all* of the structure of the domain group.

In general, for similar reasons, any homomorphism that is one-to-one preserves all of the structure of its domain group.

Now consider the homomorphism ϕ_2 , illustrated in Figure 18. It is not one-to-one: it maps the eight elements of the domain group to just two elements of the codomain group.

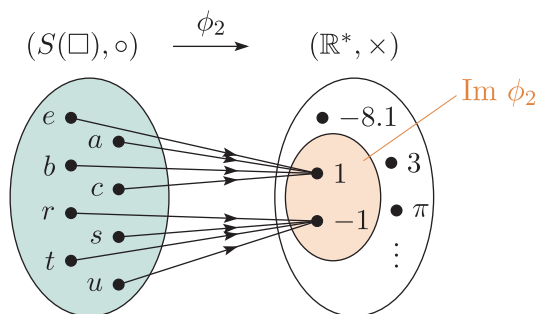


Figure 18 The homomorphism ϕ_2 and its image

It follows that this homomorphism does not preserve all of the structure of the domain group. However, it does preserve some structure, namely the structure relating to direct and indirect symmetries in the domain group, as follows.

It maps all the direct symmetries to a particular element of the codomain group, namely 1, and all the indirect symmetries to a different element of the codomain group, namely -1 , and, because it preserves composites, it does this in such a way that the structure relating to composing these two types of symmetries is preserved. For example, if we compose a direct symmetry and an indirect symmetry in the domain group then we get an indirect symmetry, and correspondingly if we compose the images of these symmetries, which are 1 and -1 respectively, in the codomain group then we get -1 , which corresponds to indirectness.

Next consider the homomorphism ϕ_3 , illustrated in Figure 19.

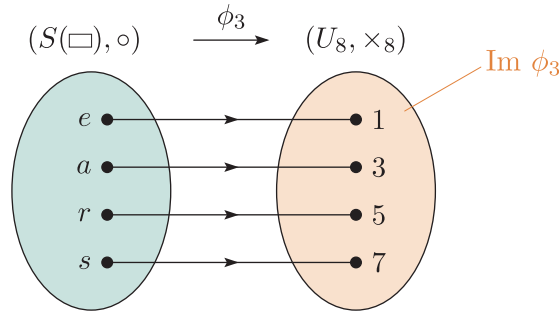


Figure 19 The homomorphism ϕ_3 and its image

This homomorphism is one-to-one, so like ϕ_1 it preserves *all* of the structure of the domain group. The domain group $S(\square)$ is isomorphic to $\text{Im } \phi_3$, which in this case (since ϕ_3 is onto) is equal to the codomain group (U_8, \times_8) .

Finally consider the homomorphism ϕ_4 , given by

$$\begin{aligned}\phi_4 : (\mathbb{R}^*, \times) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto |x|.\end{aligned}$$

It is illustrated in Figure 20, though this diagram cannot show the images of all elements in the domain group because the domain group is an infinite set.

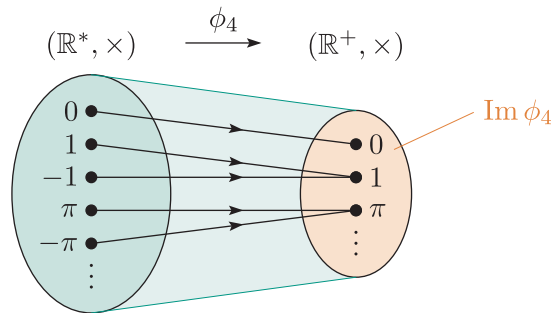


Figure 20 The homomorphism ϕ_4 and its image

Like ϕ_2 , the homomorphism ϕ_4 is not one-to-one. For example, it maps both the elements 1 and -1 of the domain group to the element 1 of the image. So it does not preserve all the structure of the domain group.

However, it does preserve some of the structure, namely the structure relating to the modulus of the elements in the domain group. It maps elements of the same modulus to the same element, regardless of whether they are positive or negative and, because it preserves composites, it does this in such a way that the structure relating to composing elements of different modulus is preserved.

You saw in the discussion above that the one-to-one homomorphisms ϕ_1 and ϕ_3 preserve *all* of the structure of their domain groups. They illustrate the following general fact.

Proposition E48

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a one-to-one homomorphism, and let θ be the mapping obtained from ϕ by shrinking the codomain of ϕ to its subgroup $\text{Im } \phi$. Then θ is an isomorphism, and hence $(G, \circ) \cong \text{Im } \phi$.

Proof Shrinking the codomain of ϕ from $(H, *)$ to its subgroup $\text{Im } \phi$ does not affect either the homomorphism property of ϕ or the fact that it is one-to-one, so θ has these properties too. However, θ is also onto, so it is an isomorphism from (G, \circ) to $\text{Im } \phi$, and hence $(G, \circ) \cong \text{Im } \phi$. ■

Proposition E48 tells us that, as mentioned in the discussion above, every one-to-one homomorphism ϕ preserves *all* of the structure of the domain group. This structure is preserved in $\text{Im } \phi$, not necessarily in the whole codomain group. (It is preserved in the whole codomain group if ϕ is also onto, that is, if ϕ is an isomorphism.)

Now let us briefly consider some particular structural features of groups that are always preserved by homomorphisms. You met several such features in Subsection 1.3, as follows:

- composites of any finite number of elements
- the identity
- inverses
- powers
- conjugates.

The next theorem states two more structural properties that are always preserved by homomorphisms.

Theorem E49

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism.

- (a) If (G, \circ) is abelian, then $(\text{Im } \phi, *)$ is abelian.
- (b) If (G, \circ) is cyclic, then $(\text{Im } \phi, *)$ is cyclic.

In particular, if (G, \circ) is generated by a , then $(\text{Im } \phi, *)$ is generated by $\phi(a)$.

Proof

- (a) Suppose that (G, \circ) is abelian. We have to show that $(\text{Im } \phi, *)$ is abelian. Let h_1, h_2 be any elements of $\text{Im } \phi$. Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. Since (G, \circ) is abelian, we have

$$g_1 \circ g_2 = g_2 \circ g_1.$$

Hence

$$\phi(g_1 \circ g_2) = \phi(g_2 \circ g_1).$$

Since ϕ is a homomorphism, this gives

$$\phi(g_1) * \phi(g_2) = \phi(g_2) * \phi(g_1);$$

that is,

$$h_1 * h_2 = h_2 * h_1.$$

This shows that $(\text{Im } \phi, *)$ is abelian.

- (b) Suppose that (G, \circ) is cyclic, generated by a . We will show that $(\text{Im } \phi, *)$ is also cyclic, generated by $\phi(a)$. Let h be any element of $\text{Im } \phi$. We have to show that h can be expressed as a power of $\phi(a)$. Now $h = \phi(g)$ for some $g \in G$. Since (G, \circ) is generated by a , we have

$$g = a^k$$

for some integer k . Hence

$$\phi(g) = \phi(a^k);$$

that is,

$$h = \phi(a^k).$$

By Proposition E43, this gives

$$h = (\phi(a))^k.$$

This expresses h as a power of $\phi(a)$. Thus $(\text{Im } \phi, *)$ is cyclic, generated by $\phi(a)$. ■

As an illustration of Theorem E49, consider the homomorphism ϕ_1 from Worked Exercise E45, shown again in Figure 21. Its domain group is $(\mathbb{Z}_4, +_4)$, which is cyclic and hence also abelian. Hence by Theorem E49 its image $\text{Im } \phi$ must also be cyclic and abelian, which indeed it is: it is the cyclic subgroup of \mathbb{Z}_8 generated by the element 2.

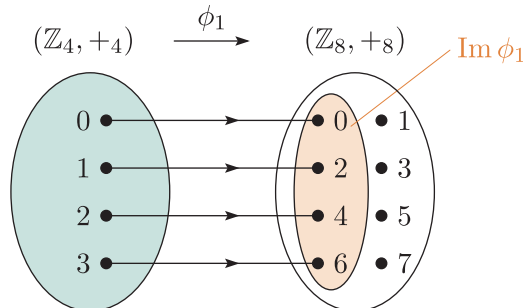


Figure 21 The homomorphism ϕ_1 and its image

Exercise E119

Explain why homomorphisms do not exist with the following properties.

- (a) Domain group $(\mathbb{Z}_{12}, +_{12})$ and image $(S(\triangle), \circ)$.
- (b) Domain group $(\mathbb{Z}_{12}, +_{12})$ and image $(S(\square), \circ)$.

The converses of the results in Theorem E49 do not hold. If the image of a homomorphism ϕ is abelian, then the domain group of ϕ may or may not be abelian. Similarly, if the image of a homomorphism ϕ is cyclic, then the domain group of ϕ may or may not be cyclic. For example, the image of the homomorphism ϕ_2 from Worked Exercise E45 is $(\{1, -1\}, \times)$, which is both abelian and cyclic, but the domain group of ϕ_2 is $(S(\square), \circ)$, which is neither abelian nor cyclic.

2.2 Kernel of a homomorphism

The definition of the kernel of a homomorphism is given below, and illustrated in Figure 22.

Definition

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. The **kernel** of ϕ is

$$\text{Ker } \phi = \{g \in G : \phi(g) = e_H\}.$$

It is the set of elements of the domain group G that are mapped by ϕ to e_H .

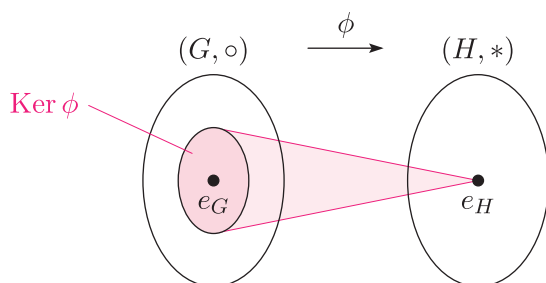


Figure 22 The kernel of a homomorphism

The kernel of a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ certainly contains e_G , as shown in Figure 22, because $\phi(e_G) = e_H$, by Proposition E41.

The definition of the kernel of a homomorphism is essentially the same as the definition of the kernel of a linear transformation, which you met in Subsection 4.2 of Unit C3. You saw earlier that every linear transformation is also a homomorphism, so this is as you would expect.

Note that the definition of a kernel applies only to homomorphisms, not to functions in general, because the codomain of a function need not contain an identity element. This contrasts with the definition of an *image*, which does apply to all functions.

Worked Exercise E46

Write down the kernel of each of the following homomorphisms.

- (a) $\phi_1 : (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_8, +_8)$
- $0 \mapsto 0$
 $1 \mapsto 2$
 $2 \mapsto 4$
 $3 \mapsto 6$
- (b) $\phi_2 : (S(\square), \circ) \longrightarrow (\mathbb{R}^*, \times)$
- $e, a, b, c \mapsto 1$
 $r, s, t, u \mapsto -1$

(These are the same homomorphisms as in Worked Exercise E45 in the previous subsection.)

Solution

- (a) The identity element of the codomain group is 0.
The only element of the domain group that is mapped to 0 by ϕ_1 is 0.
Hence
 $\text{Ker } \phi = \{0\}.$
- (b) The identity element of the codomain group is 1.
The elements of the domain group that are mapped to 1 by ϕ_2 are e, a, b and c .
Hence
 $\text{Ker } \phi = \{e, a, b, c\}.$

The kernels of the homomorphisms in Worked Exercise E46 are illustrated in Figure 23. Notice that the elements of the kernel of the homomorphism ϕ_2 are the direct symmetries in $S(\square)$. That is, $\text{Ker } \phi_2 = S^+(\square)$.

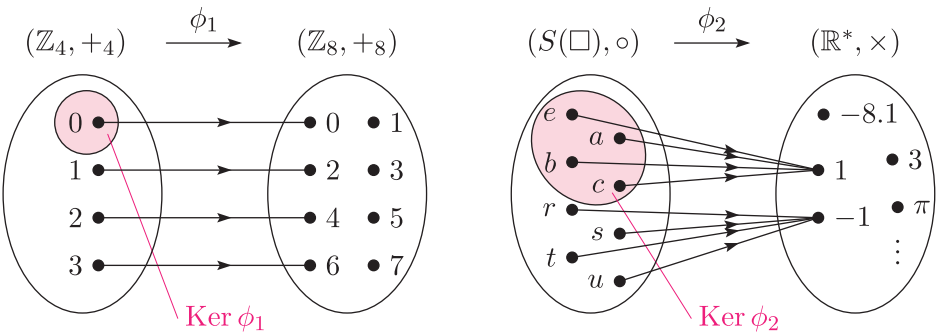


Figure 23 The kernels of the homomorphisms ϕ_1 and ϕ_2 in Worked Exercise E46

Exercise E120

For each of the following homomorphisms, write down the identity element of the codomain group, and hence write down the kernel of the homomorphism.

- (a) $\phi_3 : (S(\square), \circ) \longrightarrow (U_8, \times_8)$ (b) $\phi_4 : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^+, \times)$
- $$\begin{array}{ll} e \longmapsto 1 & x \longmapsto |x| \\ a \longmapsto 3 & \\ r \longmapsto 5 & \\ s \longmapsto 7 & \end{array}$$

(These are the same homomorphisms as in Exercise E117 in the previous subsection.)

You saw earlier that the image of a homomorphism is always a subgroup of the codomain group. The kernel has a similar property. By definition, it is a *subset* of the domain group, but in fact it is always a *subgroup* of the domain group.

To illustrate this, consider again the homomorphisms ϕ_1 , ϕ_2 , ϕ_3 and ϕ_4 from Worked Exercise E46 and Exercise E120. Their domain groups and kernels are summarised in Table 2.

Table 2 Domain groups and kernels of four homomorphisms

| Homomorphism | Domain group | Kernel |
|--------------|--------------------------|----------------|
| ϕ_1 | $(\mathbb{Z}_4, +)$ | $\{0\}$ |
| ϕ_2 | $(S(\square), \circ)$ | $S^+(\square)$ |
| ϕ_3 | $(S(\square), \circ)$ | $\{e\}$ |
| ϕ_4 | (\mathbb{R}^*, \times) | $\{1, -1\}$ |

For ϕ_1 and ϕ_3 , the kernel contains the identity element alone, so it is the trivial subgroup of the domain group. For ϕ_2 , the kernel is the subgroup $S^+(\square)$ of the domain group $S(\square)$ formed by the direct symmetries. Finally, for ϕ_4 , the kernel is the cyclic subgroup of the domain group (\mathbb{R}^*, \times) generated by -1 . So in each case the kernel is a subgroup of the domain group.

Here is a formal statement and proof of this property.

Theorem E50

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then $\text{Ker } \phi$ is a subgroup of (G, \circ) .

Proof We check that the three subgroup properties hold.

SG1 Closure

Let k_1 and k_2 be elements of $\text{Ker } \phi$. Then $\phi(k_1) = e_H$ and $\phi(k_2) = e_H$. We have to show that $k_1 \circ k_2 \in \text{Ker } \phi$.

Now

$$\begin{aligned}\phi(k_1 \circ k_2) &= \phi(k_1) * \phi(k_2) \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= e_H * e_H \\ &= e_H.\end{aligned}$$

This shows that $k_1 \circ k_2 \in \text{Ker } \phi$.

SG2 Identity

By Proposition E41 we have $\phi(e_G) = e_H$, so $e_G \in \text{Ker } \phi$.

SG3 Inverses

Let $k \in \text{Ker } \phi$. Then $\phi(k) = e_H$. We have to show that $k^{-1} \in \text{Ker } \phi$.

Now

$$\begin{aligned}\phi(k^{-1}) &= (\phi(k))^{-1} \quad (\text{by Proposition E42}) \\ &= e_H^{-1} \\ &= e_H.\end{aligned}$$

Hence $k^{-1} \in \text{Ker } \phi$.

This shows that $(\text{Ker } \phi, \circ)$ is a subgroup of (G, \circ) . ■

In fact an even stronger result than Theorem E50 holds. Not only is the kernel of a homomorphism always a subgroup of the domain group, but it is always a *normal* subgroup. You can see from Table 2 that this holds for the four homomorphisms ϕ_1, ϕ_2, ϕ_3 and ϕ_4 . For ϕ_1, ϕ_3 and ϕ_4 , the domain group is an abelian group, so every subgroup of the domain group is normal. For ϕ_2 , the domain group $S(\square)$ has order 8 and the kernel $S^+(\square)$ has order 4, so the kernel has index 2 in $S(\square)$ and is therefore normal (by Theorem E11 in Unit E1). Here is a proof of this important result.

Theorem E51

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then $\text{Ker } \phi$ is a normal subgroup of (G, \circ) .

Proof We know from Theorem E50 that $\text{Ker } \phi$ is a subgroup of (G, \circ) , so we have only to prove that $\text{Ker } \phi$ is normal in (G, \circ) . To do this we use Theorem E20 (Property B) from Unit E2 *Quotient groups and conjugacy*. (This says that a subgroup H of a group G is normal in G if and only if $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$.)

Let $k \in \text{Ker } \phi$ and let $g \in G$. We have to show that $g \circ k \circ g^{-1} \in \text{Ker } \phi$.

Now

$$\begin{aligned}
 \phi(g \circ k \circ g^{-1}) &= \phi(g) * \phi(k) * \phi(g^{-1}) \quad (\text{by Proposition E40}) \\
 &= \phi(g) * e_H * \phi(g^{-1}) \quad (\text{since } k \in \text{Ker } \phi) \\
 &= \phi(g) * \phi(g^{-1}) \\
 &= \phi(g) * (\phi(g))^{-1} \quad (\text{by Proposition E42}) \\
 &= e_H.
 \end{aligned}$$

This shows that $g \circ k \circ g^{-1} \in \text{Ker } \phi$. It follows that $(\text{Ker } \phi, \circ)$ is normal in (G, \circ) , as required. ■

The next theorem gives another important property of the kernel of a homomorphism.

Theorem E52

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then ϕ is one-to-one if and only if $\text{Ker } \phi = \{e_G\}$.

Proof ‘Only if’ part

Suppose that ϕ is one-to-one. We know that ϕ maps e_G to e_H , by Proposition E41. Since ϕ is one-to-one, it does not map any other element of G to e_H . So $\text{Ker } \phi = \{e_G\}$.

‘If’ part

Suppose that $\text{Ker } \phi = \{e_G\}$. We have to prove that ϕ is one-to-one. To do this, suppose that $x, y \in G$ with $\phi(x) = \phi(y)$. We must show that $x = y$. Composing each side of the equation $\phi(x) = \phi(y)$ on the right with $(\phi(y))^{-1}$ (in the group $(H, *)$) gives

$$\phi(x) * (\phi(y))^{-1} = \phi(y) * (\phi(y))^{-1};$$

that is,

$$\phi(x) * (\phi(y))^{-1} = e_H.$$

Hence, by Proposition E42,

$$\phi(x) * \phi(y^{-1}) = e_H.$$

Since ϕ is a homomorphism we obtain

$$\phi(x \circ y^{-1}) = e_H.$$

Therefore $x \circ y^{-1} \in \text{Ker } \phi$, and hence, since $\text{Ker } \phi = \{e_G\}$, we have

$$x \circ y^{-1} = e_G.$$

Composing both sides of this equation on the right with y (in the group (G, \circ)) then gives

$$x \circ y^{-1} \circ y = e_G \circ y;$$

that is,

$$x = y,$$

as required. This shows that ϕ is one-to-one. ■

Theorem E52 is illustrated by the homomorphisms ϕ_1 and ϕ_2 from Worked Exercise E46, which are shown again in Figure 24. The homomorphism ϕ_1 is one-to-one and its kernel consists of the identity element alone, whereas the homomorphism ϕ_2 is not one-to-one and its kernel contains other elements as well as the identity element.

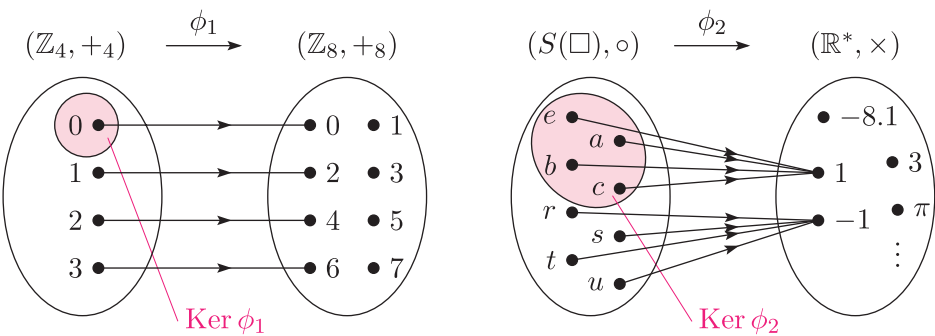


Figure 24 The kernels of the homomorphisms ϕ_1 and ϕ_2 from Worked Exercise E46



Lev Semyonovich Pontryagin

As mentioned in Unit C3, the first person to use the term *kernel* in an algebraic context was Lev Semyonovich Pontryagin (1908–1988), who used it in a paper published in 1931. Pontryagin’s book *Topological Groups* (1938), translated into English in 1946, was extremely influential and is today recognised as a classic in its field. Later in his career Pontryagin turned to problems in applied mathematics.

Kernels of homomorphisms and normal subgroups

We end this subsection with an illuminating theorem that links kernels of homomorphisms and normal subgroups.

Consider any group (G, \circ) . By Theorem E51, the kernel of any homomorphism with domain group (G, \circ) is a normal subgroup of (G, \circ) . In fact the converse of this statement is also true: any normal subgroup of (G, \circ) is the kernel of some homomorphism with domain group (G, \circ) . So we have the following theorem.

Theorem E53
Let K be a subgroup of a group (G, \circ) . Then K is normal in G if and only if K is the kernel of a homomorphism with domain group G .

Proof

‘If’ part

By Theorem E51, if K is the kernel of a homomorphism with domain group G then K is normal in G .

‘Only if’ part

Suppose that K is normal in G . We have to show that K is the kernel of a homomorphism with domain group G .

Let ϕ be the mapping

$$\begin{aligned}\phi : (G, \circ) &\longrightarrow (G/K, \cdot) \\ x &\longmapsto xK.\end{aligned}$$

The domain of this mapping is the group G , and its codomain is the quotient group G/K , which exists because K is normal in G . So the elements of the codomain group are the cosets of K in G , and the binary operation in the codomain group is set composition, which as usual we denote by the symbol \cdot .

The mapping ϕ is a homomorphism, because if $x, y \in G$ then

$$\begin{aligned}\phi(x \circ y) &= (x \circ y)K \quad (\text{by the definition of } \phi) \\ &= (xK) \cdot (yK) \quad (\text{by Theorem E1 in Unit E2}) \\ &= \phi(x) \cdot \phi(y) \quad (\text{by the definition of } \phi).\end{aligned}$$

Also, the identity element of the quotient group G/K is K , so

$$\begin{aligned}\text{Ker } \phi &= \{x \in G : \phi(x) = K\} \\ &= \{x \in G : xK = K\} \\ &= K.\end{aligned}$$

Hence ϕ is a homomorphism with kernel K , as required. ■

Given a group (G, \circ) and one of its normal subgroups K , there are many homomorphisms with domain group (G, \circ) and kernel K other than the one defined in the proof of Theorem E53.

Theorem E53 shows that kernels of homomorphisms and normal subgroups are essentially the same objects.

2.3 Finding images and kernels

You have already found the images and kernels of some homomorphisms in the previous two subsections. This subsection provides further practice in doing this, including in some more complicated cases such as when the domain group and/or codomain group are matrix groups.

Keep in mind that the image of a homomorphism is a subgroup of the *codomain group*, and the kernel is a subgroup of the *domain group*.

Remember too that usually the first step in finding the kernel of a homomorphism is to identify the identity element of the codomain group. Also, by Theorem E52, if a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ is one-to-one, then its kernel is just $\{e_G\}$.

First try the following exercise.

Exercise E121

Find the image and kernel of each of the following homomorphisms.

- (a) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$ (b) $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \times)$
 $n \longmapsto 3 \times_6 n$ $x \longmapsto e^x$
- (c) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$
 $x \longmapsto 1$

(You saw that the mappings in parts (a) and (b) are homomorphisms in Exercise E107(c) in Subsection 1.2 and Exercise E102 in Subsection 1.1, respectively. The mapping in part (c) is a homomorphism by Proposition E38.)

If the domain group of a homomorphism is an infinite set, then we often need an algebraic argument to find its image and kernel, as demonstrated next.


Worked Exercise E47

Find the image and kernel of the homomorphism


$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z|.\end{aligned}$$

(This mapping was shown to be a homomorphism in Worked Exercise E41.)

Solution



 To find the image, we apply the definition, which says that for a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$,

$$\text{Im } \phi = \{\phi(g) : g \in G\}.$$

For the homomorphism in the question the domain group G is \mathbb{C}^* . We will denote a general element of \mathbb{C}^* by z , as in the question. 

The image is

$$\begin{aligned}\text{Im } \phi &= \{\phi(z) : z \in \mathbb{C}^*\} \\ &= \{|z| : z \in \mathbb{C}^*\}\end{aligned}$$

 So $\text{Im } \phi$ consists of all the values taken by $|z|$ as z takes all possible values in \mathbb{C}^* . That is, $\text{Im } \phi$ consists of all the positive real numbers. 

$$= \mathbb{R}^+.$$

☁ To find the kernel, we first identify the identity element of the codomain group. ☁

The identity element of the codomain group (\mathbb{R}^*, \times) is 1.

☁ Then we apply the definition of the kernel, which says that for a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$,

$$\text{Ker } \phi = \{g \in G : \phi(g) = e_H\}. \quad \text{☁}$$

Hence the kernel is

$$\begin{aligned} \text{Ker } \phi &= \{z \in \mathbb{C}^* : \phi(z) = 1\} \\ &= \{z \in \mathbb{C}^* : |z| = 1\} \end{aligned}$$

☁ We can simplify this specification slightly. The set of *all non-zero* complex numbers with modulus 1 is the same as the set of *all* complex numbers with modulus 1. ☁

$$= \{z \in \mathbb{C} : |z| = 1\}.$$

☁ This specification is acceptably simple. Since $\text{Ker } \phi$ is a subset of \mathbb{C} , which has a geometric representation as the complex plane, we should give a geometric description of $\text{Ker } \phi$ as well as the algebraic specification above. ☁

So $\text{Ker } \phi$ is the set of all complex numbers that lie on the circle with centre 0 and radius 1 in the complex plane; that is, it is the unit circle.

Exercise E122

Show that the mapping

$$\begin{aligned} \phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto 7n \end{aligned}$$

is a homomorphism, and find its image and kernel.

The next worked exercise involves finding the image and kernel of a homomorphism whose domain group is an infinite matrix group. Remember that throughout this book we use L to denote the group of invertible 2×2 lower triangular matrices with real entries, and D to denote the group of invertible 2×2 diagonal matrices with real entries, each under matrix multiplication:

$$\begin{aligned} L &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0 \right\}, \\ D &= \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}, ad \neq 0 \right\}. \end{aligned}$$

Worked Exercise E48

Find the image and kernel of the homomorphism

$$\begin{aligned}\phi : (L, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto a^2 d^2.\end{aligned}$$


(You saw that this mapping is a homomorphism in Exercise E111(b).)

Solution

First we find the image.



 Apply the definition of the image,

$$\text{Im } \phi = \{\phi(g) : g \in G\},$$



to the particular homomorphism ϕ here. A general element of the domain group L is $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$, where $a, c, d \in \mathbb{R}$ and $ad \neq 0$. 

We have

$$\begin{aligned}\text{Im } \phi &= \left\{ \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L \right\} \\ &= \left\{ a^2 d^2 : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L \right\}.\end{aligned}$$

 Simplify the condition after the colon. (Remember that the colon means ‘such that’.) What the condition tells us about the values taken by a and d is that $a, d \in \mathbb{R}$ with $ad \neq 0$. 

$$= \{a^2 d^2 : a, d \in \mathbb{R}, ad \neq 0\}.$$

 As a and d run through all values in \mathbb{R} such that $ad \neq 0$, the expression $a^2 d^2$ takes all possible *positive* values in \mathbb{R} . 

$$= \mathbb{R}^+.$$

Now we find the kernel.



 First identify the identity element of the codomain group. Then apply the definition of the kernel,

$$\text{Ker } \phi = \{g \in G : \phi(g) = e_H\},$$

to the particular homomorphism ϕ here. 

The codomain group is (\mathbb{R}^*, \times) , which has identity element 1, so

$$\text{Ker } \phi = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = 1 \right\}.$$

 Simplify the condition after the colon. We can do this outside the set notation, for brevity. 

Now

$$\begin{aligned}
 \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = 1 &\iff a^2 d^2 = 1 \\
 &\iff (ad)^2 = 1 \\
 &\iff ad = \pm 1 \\
 &\iff d = \pm 1/a.
 \end{aligned}$$

Therefore

$$\text{Ker } \phi = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : d = \pm 1/a \right\}$$

 We can simplify this expression for $\text{Ker } \phi$ further by rewriting

$$\begin{aligned}
 \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \dots \right\} &\text{ as } \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0, \dots \right\}. \quad \text{...} \\
 &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0, d = \pm 1/a \right\} \\
 &= \left\{ \begin{pmatrix} a & 0 \\ c & \pm 1/a \end{pmatrix} : a, c \in \mathbb{R}, a \neq 0 \right\}.
 \end{aligned}$$

The expression for $\text{Ker } \phi$ obtained in the worked exercise above could also be written as

$$\left\{ \begin{pmatrix} a & 0 \\ c & \pm 1/a \end{pmatrix} : a \in \mathbb{R}^*, c \in \mathbb{R} \right\}.$$

Exercise E123

Find the image and kernel of the homomorphism

$$\begin{aligned}
 \phi : (L, \times) &\longrightarrow (L, \times) \\
 \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix}.
 \end{aligned}$$

(You saw that this mapping is a homomorphism in Worked Exercise E44 in Subsection 1.2.)

Exercise E124

Find the kernel of the homomorphism

$$\begin{aligned}
 \phi : (L, \times) &\longrightarrow (D, \times) \\
 \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.
 \end{aligned}$$

(Its image is found in the next worked exercise. You saw that this mapping is a homomorphism in Exercise E109(a) in Subsection 1.2.)

The next worked exercise reminds you about a different type of algebraic argument that is sometimes useful when you want to find the image of a homomorphism. If you suspect that the image is the *whole codomain group* – that is, the homomorphism is *onto* – then you can verify this by using an algebraic argument to prove that every element of the codomain group is the image of some element of the domain group.



Worked Exercise E49

Find the image of the homomorphism

$$\begin{aligned}\phi : (L, \times) &\longrightarrow (D, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.\end{aligned}$$

(You were asked to find the kernel of this homomorphism in Exercise E124.)



Solution

 We suspect that this homomorphism is onto, so we try to use an algebraic argument to prove that it is. We have to show that every element of the codomain group is the image under ϕ of some element of the domain group. 

We show that ϕ is onto. A general element of the codomain group (D, \times) is

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},$$

where $a, d \in \mathbb{R}$ and $ad \neq 0$.

 Find *any* element of the domain group that is mapped by ϕ to this matrix. Remember to check that the element that you have found satisfies all the conditions to be in the domain group. 

The matrix

$$\begin{pmatrix} a & 0 \\ 1 & d \end{pmatrix}$$

is an element of the domain group (L, \times) , because it is lower triangular and its determinant is ad which is non-zero, and

$$\phi \begin{pmatrix} a & 0 \\ 1 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

Thus ϕ is onto, and hence

$$\text{Im } \phi = (D, \times).$$

Exercise E125

Show that the following homomorphism is onto and hence write down its image:

$$\begin{aligned}\phi : (L, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \frac{a}{d}.\end{aligned}$$

(You saw that this mapping is a homomorphism in Exercise E111(c) in Subsection 1.2.)



Finally, here is one more possible approach to keep in mind when you want to find the image or kernel of a homomorphism. You could try making an informed guess about what the image or kernel is, and then confirm your guess by applying Strategy A1 from Unit A1. This strategy says that to show that two sets are equal, show that each set is a subset of the other. Thus if you think that $\text{Im } \phi$ is a particular set S , say, then you can confirm this by showing that $\text{Im } \phi \subseteq S$ and $S \subseteq \text{Im } \phi$. Here is an example; it involves the same homomorphism as in Worked Exercise E48, but it determines the image of the homomorphism in the way just described.

Worked Exercise E50

Find the image of the homomorphism

$$\begin{aligned}\phi : (L, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto a^2 d^2.\end{aligned}$$

Solution

 Make an informed guess about what the image is, then confirm it. The specification of ϕ suggests that $\text{Im } \phi = \mathbb{R}^+$. 

We show that $\text{Im } \phi = \mathbb{R}^+$.

First we show that $\text{Im } \phi \subseteq \mathbb{R}^+$. Let $r \in \text{Im } \phi$. Then

$$r = \phi \left(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \right),$$

where $a, c, d \in \mathbb{R}$ and $ad \neq 0$. This gives

$$r = a^2 d^2.$$

Since $a, d \in \mathbb{R}$ and $ad \neq 0$, it follows that $r > 0$ and hence $r \in \mathbb{R}^+$. Therefore $\text{Im } \phi \subseteq \mathbb{R}^+$.

Now we show that $\mathbb{R}^+ \subseteq \text{Im } \phi$. Let $r \in \mathbb{R}^+$. Then r is the image under ϕ of the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{r} \end{pmatrix},$$

since

$$\phi \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{r} \end{pmatrix} = 1^2 (\sqrt{r})^2 = r.$$

Also

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{r} \end{pmatrix} \in L$$

because it is of the form

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

with $a = 1$, $c = 0$, $d = \sqrt{r}$ and $ad = 1\sqrt{r} = \sqrt{r} \neq 0$. Hence $r \in \text{Im } \phi$. Therefore $\mathbb{R}^+ \subseteq \text{Im } \phi$.

Since $\text{Im } \phi \subseteq \mathbb{R}^+$ and $\mathbb{R}^+ \subseteq \text{Im } \phi$, it follows that $\text{Im } \phi = \mathbb{R}^+$.

Exercise E126

Use the method of Worked Exercise E50 to show that the image of the homomorphism

$$\begin{aligned} \phi : (\mathbb{R}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ x &\longmapsto x^2 \end{aligned}$$

is \mathbb{R}^+ .

(You saw that ϕ is a homomorphism in Exercise E107(a) in Subsection 1.2.)

3 The First Isomorphism Theorem

This section leads up to and covers the *First Isomorphism Theorem*, an important theorem in group theory that links the ideas of homomorphisms and quotient groups.

3.1 Cosets of the kernel of a homomorphism

You saw in the last section that the kernel of a homomorphism is a *normal* subgroup of its domain group. Thus the left cosets of the kernel in the domain group are the same as its right cosets, and we refer to them simply as cosets. In this subsection you will meet an important property of the cosets of the kernel of a homomorphism.

Here is an example that illustrates this property. Consider the mapping

$$\begin{aligned}\phi : (\mathbb{Z}_{12}, +_{12}) &\longrightarrow (\mathbb{Z}_{12}, +_{12}) \\ n &\longmapsto 3 \times_{12} n.\end{aligned}$$

This is a homomorphism because, for any $m, n \in \mathbb{Z}_{12}$,

$$\begin{aligned}\phi(m +_{12} n) &= 3 \times_{12} (m +_{12} n) \\ &= (3 \times_{12} m) +_{12} (3 \times_{12} n) \\ &= \phi(m) +_{12} \phi(n).\end{aligned}$$

Let us find its kernel. The identity element of the codomain group is 0, so

$$\begin{aligned}\text{Ker } \phi &= \{n \in \mathbb{Z}_{12} : \phi(n) = 0\} \\ &= \{n \in \mathbb{Z}_{12} : 3 \times_{12} n = 0\} \\ &= \{0, 4, 8\}.\end{aligned}$$

We will now find the cosets of $\text{Ker } \phi$ in the domain group $(\mathbb{Z}_{12}, +_{12})$. Using our usual method for finding cosets, we find that they are

$$\begin{aligned}\text{Ker } \phi &= \{0, 4, 8\}, \\ 1 + \text{Ker } \phi &= \{1, 5, 9\}, \\ 2 + \text{Ker } \phi &= \{2, 6, 10\}, \\ 3 + \text{Ker } \phi &= \{3, 7, 11\}.\end{aligned}$$

Let us now find the images under ϕ of the elements of the domain group $(\mathbb{Z}_{12}, +_{12})$, one coset at a time.

The image under ϕ of each element of $\text{Ker } \phi$ itself is, of course, 0.

Now we find the images of the elements in the second coset above:

$$\phi(1) = 3, \quad \phi(5) = 3, \quad \phi(9) = 3.$$

Each element of this coset has the *same* image, namely 3.

A similar property is true for each of the other two cosets:

$$\begin{aligned}\phi(2) &= \phi(6) = \phi(10) = 6, \\ \phi(3) &= \phi(7) = \phi(11) = 9.\end{aligned}$$

Thus whenever two elements of the domain group $(\mathbb{Z}_{12}, +_{12})$ lie in the *same* coset of $\text{Ker } \phi$, they have the *same* image under ϕ , whereas whenever they lie in *different* cosets, they have *different* images. This is illustrated in Figure 25.

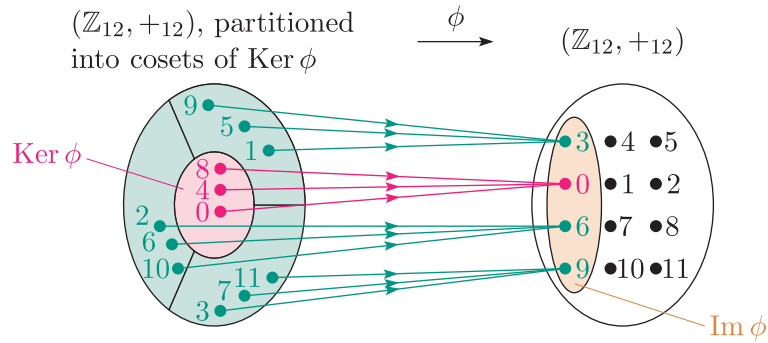


Figure 25 The homomorphism $\phi : (\mathbb{Z}_{12}, +_{12}) \longrightarrow (\mathbb{Z}_{12}, +_{12})$ with rule $n \longmapsto 3 \times_{12} n$

This finding, for this particular homomorphism ϕ , is a particular example of the following general theorem.

Theorem E54

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism, and let x and y be any elements of G . Then

x and y have the same image under ϕ

if and only if

x and y lie in the same coset of $\text{Ker } \phi$ in G .

Proof

‘If’ part

Suppose that x and y lie in the same coset of $\text{Ker } \phi$ in G . We have to show that $\phi(x) = \phi(y)$.

Since x and y lie in the same coset of $\text{Ker } \phi$ in G , we have

$$y \in x \text{Ker } \phi.$$

Hence there is an element k in $\text{Ker } \phi$ such that

$$y = x \circ k.$$

Therefore

$$\begin{aligned} \phi(y) &= \phi(x \circ k) \\ &= \phi(x) * \phi(k) \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= \phi(x) * e_H \quad (\text{since } k \in \text{Ker } \phi) \\ &= \phi(x), \end{aligned}$$

as required.

‘Only if’ part

Suppose that $\phi(x) = \phi(y)$. We have to show that x and y lie in the same coset of $\text{Ker } \phi$ in G .

Consider the image of the element $x^{-1} \circ y$ under ϕ . We have

$$\begin{aligned}\phi(x^{-1} \circ y) &= \phi(x^{-1}) * \phi(y) \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= (\phi(x))^{-1} * \phi(y) \quad (\text{by Proposition E42}) \\ &= (\phi(x))^{-1} * \phi(x) \quad (\text{since } \phi(x) = \phi(y)) \\ &= e_H.\end{aligned}$$

Thus $x^{-1} \circ y$ belongs to $\text{Ker } \phi$. Hence there is an element k in $\text{Ker } \phi$ such that

$$x^{-1} \circ y = k.$$

Composing both sides of this equation on the left by x gives

$$y = x \circ k,$$

which shows that

$$y \in x \text{Ker } \phi.$$

That is, x and y lie in the same coset of $\text{Ker } \phi$, as required. ■

Theorem E54 tells us that, for any homomorphism, the sets of elements in the domain group that have the same image are precisely the cosets of the kernel. This means that

if we collect together the domain group elements according to their images under the homomorphism, then we have the cosets of the kernel;

and that, conversely,

if we find the cosets of the kernel, then we have the sets of domain group elements that have the same image under the homomorphism.

In the next exercise you are asked to check this for a particular homomorphism ϕ similar to the one that was used as an example at the start of this subsection.

Exercise E127

Consider the mapping

$$\begin{aligned}\phi : (\mathbb{Z}_{12}, +_{12}) &\longrightarrow (\mathbb{Z}_{12}, +_{12}) \\ n &\longmapsto 2 \times_{12} n.\end{aligned}$$

- (a) Show that ϕ is a homomorphism.
- (b) Find $\text{Ker } \phi$ and its cosets in $(\mathbb{Z}_{12}, +_{12})$.
- (c) Find the partition of \mathbb{Z}_{12} obtained by collecting together the elements of \mathbb{Z}_{12} that have the same image under ϕ . Check that this partition is the same as that found in part (b).

Theorem E54 applies to homomorphisms with infinite domain groups and/or infinite codomain groups, as well as to those with finite domain groups and finite codomain groups, as illustrated in the next exercise.

Exercise E128

Consider the mapping

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}_5, +_5) \\ k &\longmapsto k_{(\bmod 5)}.\end{aligned}$$

It is a homomorphism by Proposition E37 in Subsection 1.2. (Remember that, in this unit, the notation $k_{(\bmod n)}$ denotes the integer in \mathbb{Z}_n that is congruent to k modulo n .)

- Find $\text{Ker } \phi$ and its cosets in $(\mathbb{Z}, +)$.
- Find the partition of \mathbb{Z} obtained by collecting together elements of \mathbb{Z} that have the same image under ϕ . Check that this partition is the same as that in part (a).

The following theorem from Subsection 2.2 can be viewed as a corollary of Theorem E54, as shown by its alternative proof below.

Theorem E52

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then ϕ is one-to-one if and only if $\text{Ker } \phi = \{e_G\}$.

Proof (using Theorem E54)

‘If’ part

Suppose that $\text{Ker } \phi = \{e_G\}$. Then each coset of $\text{Ker } \phi$ consists of a single element (since by Proposition E3 in Unit E1 each coset contains the same number of elements as $\text{Ker } \phi$). So, by Theorem E54, each element of G has a distinct image under ϕ . That is, ϕ is one-to-one.

‘Only if’ part

Suppose that ϕ is one-to-one. Then each element of G has a distinct image under ϕ . So, by Theorem E54, each coset of $\text{Ker } \phi$, and in particular $\text{Ker } \phi$ itself, contains only a single element. The single element of $\text{Ker } \phi$ is e_G , since certainly $e_G \in \text{Ker } \phi$. Thus $\text{Ker } \phi = \{e_G\}$. ■

3.2 The First Isomorphism Theorem

In this subsection you will meet the *First Isomorphism Theorem*, an important theorem in group theory. There is also a *Second Isomorphism Theorem* and a *Third Isomorphism Theorem* in group theory, but these theorems are outside the scope of this module.

To understand what the First Isomorphism Theorem tells us, consider any homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$. You have seen that $\text{Ker } \phi$ is a normal subgroup of the domain group (G, \circ) , and that the sets of elements of (G, \circ) that have the same image under ϕ are precisely the cosets of $\text{Ker } \phi$ in (G, \circ) . It follows that we can use the homomorphism ϕ to define a new mapping, say f , whose domain is the set of cosets of $\text{Ker } \phi$ in (G, \circ) , whose codomain is $\text{Im } \phi$, and whose rule is

coset \longmapsto element of $\text{Im } \phi$ that is the image under ϕ of each element of
the coset.

This mapping f is illustrated in Figure 26. Note in particular that the elements of its domain are *whole cosets*, not individual elements of (G, \circ) .

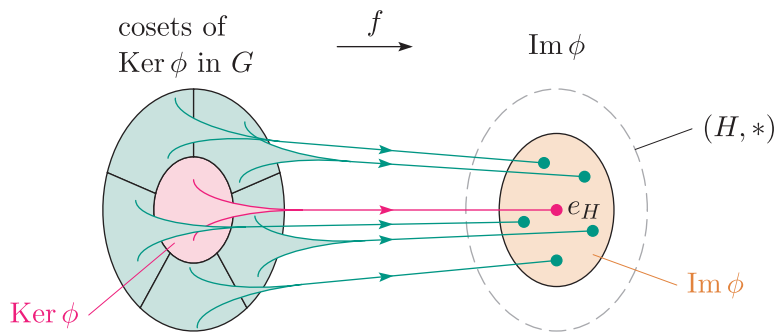


Figure 26 The mapping f obtained from the homomorphism ϕ

Since the cosets of $\text{Ker } \phi$ are the elements of the quotient group $G/\text{Ker } \phi$, and $\text{Im } \phi$ is a group, the domain and codomain of the mapping f are both *groups*. The First Isomorphism Theorem states that this mapping f is in fact always an *isomorphism*. Thus, for any homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$, the quotient group $G/\text{Ker } \phi$ is isomorphic to $\text{Im } \phi$.

For instance, consider the homomorphism ϕ that was used as an example at the start of the previous subsection:

$$\begin{aligned}\phi : (\mathbb{Z}_{12}, +_{12}) &\longrightarrow (\mathbb{Z}_{12}, +_{12}) \\ n &\longmapsto 3 \times_{12} n.\end{aligned}$$

You saw that for this homomorphism the cosets of $\text{Ker } \phi$ are

$$\{0, 4, 8\}, \quad \{1, 5, 9\}, \quad \{2, 6, 10\}, \quad \{3, 7, 11\}.$$

You also saw that ϕ maps all the elements of the first coset (which is $\text{Ker } \phi$ itself) to 0, all the elements of the second coset to 3, all the elements of the third coset to 6 and all the elements of the fourth coset to 9. The mapping f obtained from ϕ as described above is therefore

$$\begin{aligned} f : \mathbb{Z}_{12} / \text{Ker } \phi &\longrightarrow \text{Im } \phi \\ \{0, 4, 8\} &\longmapsto 0 \\ \{1, 5, 9\} &\longmapsto 3 \\ \{2, 6, 10\} &\longmapsto 6 \\ \{3, 7, 11\} &\longmapsto 9. \end{aligned}$$

It is illustrated in Figure 27.

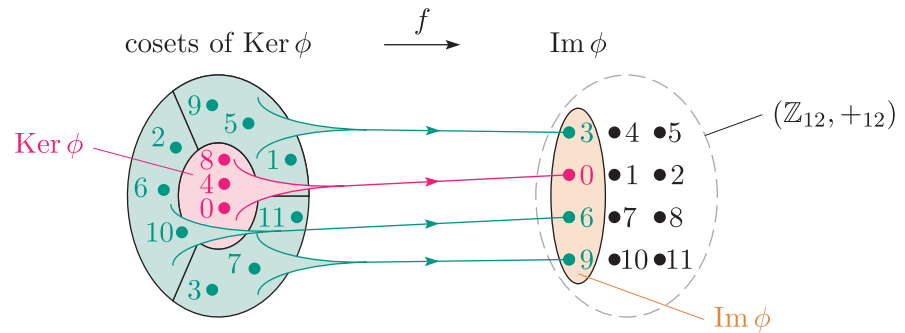


Figure 27 The mapping f obtained from the homomorphism $\phi : (\mathbb{Z}_{12}, +_{12}) \longrightarrow (\mathbb{Z}_{12}, +_{12})$ with rule $n \mapsto 3 \times_{12} n$

The First Isomorphism Theorem tells us that this mapping f is in fact an isomorphism, and hence $\mathbb{Z}_{12} / \text{Ker } \phi \cong \text{Im } \phi$; that is,

$$\mathbb{Z}_{12} / \text{Ker } \phi \cong (\{0, 3, 6, 9\}, +_{12}).$$

Here is the formal statement and proof of the First Isomorphism Theorem.

Theorem E55 First Isomorphism Theorem

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then the mapping

$$\begin{aligned} f : G / \text{Ker } \phi &\longrightarrow \text{Im } \phi \\ x \text{Ker } \phi &\longmapsto \phi(x) \end{aligned}$$

is an isomorphism, so

$$G / \text{Ker } \phi \cong \text{Im } \phi.$$

Proof In this proof we will denote $\text{Ker } \phi$ simply by K , for brevity.

The mapping f maps each coset of K to the image under ϕ of any element x of the coset. This is a valid definition of a mapping because, by Theorem E54, all the elements of a coset of K have the *same* image under ϕ . To show that f is an isomorphism, we have to show that it is one-to-one and onto and that it has the homomorphism property.

Theorem E54 tells us that elements from *different* cosets of K have *different* images under ϕ , so f is one-to-one.

Also, f is onto, because each element $\phi(x)$ of $\text{Im } \phi$ is the image under f of the coset xK .

It remains to prove that f has the homomorphism property. Let xK and yK be cosets in G/K . We have to show that

$$f(xK \cdot yK) = f(xK) * f(yK)$$

where \cdot denotes set composition. Now

$$\begin{aligned} f(xK \cdot yK) &= f((x \circ y)K) \quad (\text{by Theorem E1 in Unit E2}) \\ &= \phi(x \circ y) \quad (\text{by the definition of } f) \\ &= \phi(x) * \phi(y) \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= f(xK) * f(yK) \quad (\text{by the definition of } f). \end{aligned}$$

Hence f has the homomorphism property.

Thus f is an isomorphism from the quotient group G/K to $\text{Im } \phi$.
Therefore $G/K \cong \text{Im } \phi$. ■

The First Isomorphism Theorem is illustrated in Figure 28. This diagram shows a homomorphism ϕ and the isomorphism f obtained from ϕ as specified in the theorem. (In the diagram, as in earlier diagrams, $\text{Ker } \phi$ is shown as having finitely many cosets in the domain group (G, \circ) , but of course there could be infinitely many.)

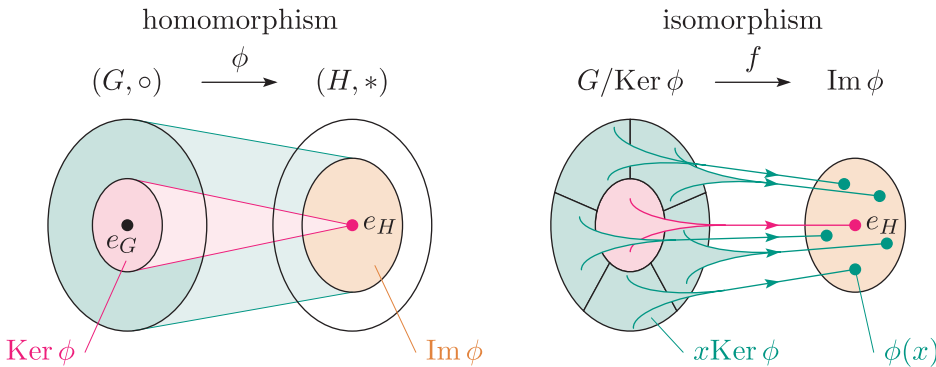


Figure 28 A homomorphism ϕ and the isomorphism f obtained from it

In the rest of this subsection we will look at one way in which we can apply the First Isomorphism Theorem, as follows.

You have seen that if N is a normal subgroup of a group G , then it can be helpful to identify a familiar, standard group that is isomorphic to the quotient group G/N . Since isomorphic groups have the same structure, this can give us useful information about the quotient group. There is a list of standard groups, both finite and infinite, in the module Handbook.

We can sometimes use the First Isomorphism Theorem to help us identify a familiar, standard group that is isomorphic to a quotient group $G/\text{Ker } \phi$, where $\phi : (G, \circ) \rightarrow (H, *)$ is a homomorphism. Here is an example.

Worked Exercise E51

Consider the mapping

$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z|.\end{aligned}$$

You saw that this mapping is a homomorphism in Worked Exercise E41 in Subsection 1.2. You also saw in Worked Exercise E47 in Subsection 2.3 that



$$\text{Im } \phi = \mathbb{R}^+$$

and

$$\text{Ker } \phi = \{z \in \mathbb{C} : |z| = 1\}.$$

State a standard group isomorphic to the quotient group $\mathbb{C}^* / \text{Ker } \phi$.

Solution

 Use the First Isomorphism Theorem. Remember that $\text{Im } \phi$ is a subgroup of the codomain group, so it has the same binary operation as the codomain group. 

By the First Isomorphism Theorem,

$$\mathbb{C}^* / \text{Ker } \phi \cong \text{Im } \phi,$$

so

$$\mathbb{C}^* / \text{Ker } \phi \cong (\mathbb{R}^+, \times).$$

So a standard group isomorphic to $\mathbb{C}^* / \text{Ker } \phi$ is (\mathbb{R}^+, \times) .

Exercise E129

Consider the mapping

$$\begin{aligned}\phi : (\mathbb{R}^2, +) &\longrightarrow (\mathbb{R}, +) \\ (x, y) &\longmapsto x + y.\end{aligned}$$

- Show that ϕ is a homomorphism.
- Find $\text{Im } \phi$ and $\text{Ker } \phi$.
- State a standard group isomorphic to the quotient group $\mathbb{R}^2 / \text{Ker } \phi$.

Exercise E130

Consider the following mapping:

$$\begin{aligned}\phi : (L, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto ad.\end{aligned}$$

(This mapping ϕ maps each matrix in L to its determinant.)

- (a) Show that ϕ is a homomorphism.
- (b) Find $\text{Im } \phi$ and $\text{Ker } \phi$.
- (c) State a standard group isomorphic to the quotient group $L/\text{Ker } \phi$.

In each of Worked Exercise E51 and Exercises E129 and E130, we found a standard group isomorphic to a quotient group $G/\text{Ker } \phi$ by finding $\text{Im } \phi$ and then using the fact that $G/\text{Ker } \phi \cong \text{Im } \phi$, by the First Isomorphism Theorem. In these cases, this gave us an immediate answer because $\text{Im } \phi$ *was itself* a standard group.

When $\text{Im } \phi$ is not a standard group, we may still be able to find a standard group isomorphic to $G/\text{Ker } \phi$ by finding a standard group isomorphic to $\text{Im } \phi$; this group will then, in turn, be isomorphic to $G/\text{Ker } \phi$. This is illustrated in the next worked exercise and in the exercise that follows it.

Worked Exercise E52

Consider the following mapping:

$$\begin{aligned}\phi : (L, \times) &\longrightarrow (L, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix}.\end{aligned}$$

You saw that this mapping is a homomorphism in Worked Exercise E44 in Subsection 1.2, and in Exercise E123 in Subsection 2.3 you saw that its image and kernel are

$$\text{Im } \phi = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} : r \in \mathbb{R}^+ \right\}$$

and

$$\text{Ker } \phi = \left\{ \begin{pmatrix} a & 0 \\ c & \pm 1 \end{pmatrix} : a, c \in \mathbb{R}, a \neq 0 \right\}.$$

Find a standard group isomorphic to the quotient group $L/\text{Ker } \phi$.

Solution

By the First Isomorphism Theorem, the quotient group $L/\text{Ker } \phi$ is isomorphic to $\text{Im } \phi$.

Here $\text{Im } \phi$, given in the question, is not a standard group. We guess that $\text{Im } \phi \cong (\mathbb{R}^+, \times)$ by considering the expression for $\text{Im } \phi$.

We now show that $\text{Im } \phi$ is isomorphic to (\mathbb{R}^+, \times) .

To do this, we show that there is an isomorphism, say θ , from $\text{Im } \phi$ to (\mathbb{R}^+, \times) .

Consider the mapping

$$\theta : \text{Im } \phi \longrightarrow \mathbb{R}^+ \\ \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \longmapsto r.$$

This mapping is one-to-one, because if

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$$

are elements of $\text{Im } \phi$ such that $\theta(\mathbf{A}) = \theta(\mathbf{B})$, then $r = s$ by the definition of θ and hence $\mathbf{A} = \mathbf{B}$.

It is also onto, because if $r \in \mathbb{R}^+$ then r is the image under θ of the element

$$\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}$$

of $\text{Im } \phi$.

Finally, θ has the homomorphism property because, for all $r, s \in \mathbb{R}^+$,

$$\begin{aligned} \theta \left(\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix} \right) &= \theta \begin{pmatrix} 1 & 0 \\ 0 & rs \end{pmatrix} \\ &= rs \\ &= \theta \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \theta \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}. \end{aligned}$$

Thus θ is an isomorphism, so

$$L / \text{Ker } \phi \cong \text{Im } \phi \cong (\mathbb{R}^+, \times).$$

So a standard group isomorphic to $L / \text{Ker } \phi$ is (\mathbb{R}^+, \times) .

Exercise E131

Consider the following mapping:

$$\phi : (L, \times) \longrightarrow (L, \times) \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} 1/a & 0 \\ 0 & 1 \end{pmatrix}.$$

- Show that ϕ is a homomorphism.
- Find $\text{Im } \phi$ and $\text{Ker } \phi$.
- Find a standard group that is isomorphic to the quotient group $L / \text{Ker } \phi$.

The First Isomorphism Theorem has the following interesting corollary for *finite* groups.

Corollary E56

Let (G, \circ) be a finite group and let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then

$$|\text{Ker } \phi| \times |\text{Im } \phi| = |G|.$$

Proof Since G is finite, each coset of $\text{Ker } \phi$ in G contains the same number of elements as $\text{Ker } \phi$, and hence the order of $G/\text{Ker } \phi$ is

$$\frac{|G|}{|\text{Ker } \phi|}.$$

It follows from the First Isomorphism Theorem that the order of $G/\text{Ker } \phi$ is the same as the order of $\text{Im } \phi$. Hence

$$\frac{|G|}{|\text{Ker } \phi|} = |\text{Im } \phi|.$$

Rearranging this equation gives the equation in the statement of the corollary. ■

If (G, \circ) and $(H, *)$ are finite groups, then the following numerical relationships hold for any homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$:

$|\text{Ker}(\phi)|$ divides $|G|$ (by Lagrange's Theorem),

$|\text{Im}(\phi)|$ divides $|H|$ (by Lagrange's Theorem),

$|\text{Im}(\phi)|$ divides $|G|$ (by Corollary E56).

In particular, the order of $\text{Im } \phi$ is a common factor of the orders of the domain group (G, \circ) and the codomain group $(H, *)$.

Worked Exercise E53

Prove that the only homomorphism from A_4 (the alternating group of degree 4) to $(\mathbb{Z}_7, +_7)$ is the trivial one.

Solution

Let $\phi : A_4 \longrightarrow \mathbb{Z}_7$ be a homomorphism. By Corollary E56 and Lagrange's Theorem, the order of $\text{Im } \phi$ divides the orders of A_4 and \mathbb{Z}_7 , which are 12 and 7, respectively. But 12 and 7 have greatest common factor 1, so the order of $\text{Im } \phi$ is 1. Hence, since $\text{Im } \phi$ is a subgroup of $(\mathbb{Z}_7, +_7)$, we have $\text{Im } \phi = \{0\}$. Therefore ϕ is the trivial homomorphism

$$\begin{aligned} \phi : A_4 &\longrightarrow \mathbb{Z}_7 \\ f &\longmapsto 0. \end{aligned}$$

Exercise E132

- (a) Prove that the only homomorphism from $(\mathbb{Z}_{11}, +_{11})$ to S_3 is the trivial one.
- (b) Prove that the only homomorphism from $S(\Delta)$ to $(\mathbb{Z}_3, +_3)$ is the trivial one.

Hint: You were asked to find the normal subgroups of $S(\Delta)$ in Exercise E39 in Subsection 3.3 of Unit E2.



Bartel van der Waerden

The first time the First, Second and Third Isomorphism Theorems appeared explicitly in the context of groups was in the famous two-volume book on abstract algebra by Bartel van der Waerden (1903–1996), *Moderne Algebra*. This book was first published in 1930–1, with an English translation appearing in 1949–50, and was originally based on lectures given by Emile Artin (1898–1962) and Emmy Noether (1882–1935). Noether, who is often described as the most important woman mathematician in the history of mathematics for her work on abstract algebra and theoretical physics, had earlier published the three theorems in a slightly different context in a paper in *Mathematische Annalen* in 1927.

3.3 Infinite quotient groups of domain groups by kernels (optional)

In the previous subsection we considered some quotient groups of the form $G/\text{Ker } \phi$, where $\phi : (G, \circ) \rightarrow (H, *)$ is a homomorphism. We used the First Isomorphism Theorem to find standard groups isomorphic to these quotient groups.

In this final, optional, subsection of the unit we will look in detail at two of these quotient groups, finding their elements and considering their binary operations. These two quotient groups are further examples of *infinite* quotient groups: so far in the module you have looked in detail at just one such quotient group, namely \mathbb{R}/\mathbb{Z} , which you met in Subsection 1.2 of Unit E2. (An infinite quotient group of an infinite group of matrices was also mentioned briefly at the end of Unit E2.)

The two examples that we will look at in this subsection are those from Worked Exercise E51 and Exercise E129 in the previous subsection. In the first of these examples the domain group G of the homomorphism ϕ is (\mathbb{C}^*, \times) , and in the second it is $(\mathbb{R}^2, +)$. So in each case the domain group G has a geometric interpretation, and hence the elements of the quotient group $G/\text{Ker } \phi$, which are subsets of G , also have geometric interpretations.



Emmy Noether

Worked Exercise E54

Consider the homomorphism

$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z|.\end{aligned}$$

(You saw that this mapping is a homomorphism in Worked Exercise E41 in Subsection 1.2.)

In Worked Exercise E47 in Subsection 2.3 we found that its kernel is

$$\text{Ker } \phi = \{z \in \mathbb{C} : |z| = 1\}.$$

That is, its kernel is the unit circle in the complex plane (the circle with centre 0 and radius 1), as shown in Figure 29.

- Find the particular cosets $2\text{Ker } \phi$ and $3i\text{Ker } \phi$ and describe them geometrically.
- Find the general coset $a\text{Ker } \phi$, where $a \in \mathbb{C}^*$, and describe it geometrically.
- Hence specify the elements of the quotient group $\mathbb{C}^*/\text{Ker } \phi$, and describe them geometrically.

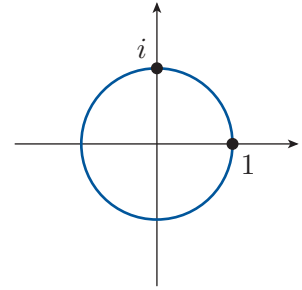


Figure 29 The unit circle in the complex plane

Solution

- (a) The coset $2\text{Ker } \phi$ is obtained by multiplying each element of $\text{Ker } \phi$ by 2.

We have

$$2\text{Ker } \phi = \{2z : z \in \text{Ker } \phi\}$$

Since $\text{Ker } \phi$ consists of all the complex numbers with modulus 1, we can see from this specification of the coset $2\text{Ker } \phi$ that it will consist of all the complex numbers with modulus 2. We can also prove this algebraically, as below. The specification of $\text{Ker } \phi$, given in the question, tells us that the condition $z \in \text{Ker } \phi$ is equivalent to the conditions $z \in \mathbb{C}$, $|z| = 1$.

$$= \{2z : z \in \mathbb{C}, |z| = 1\}$$

To obtain z rather than $2z$ in front of the colon, replace $2z$ by z everywhere.

$$= \{z : z/2 \in \mathbb{C}, |z/2| = 1\}$$

Simplify both conditions. The condition $z/2 \in \mathbb{C}$ says the same as $z \in \mathbb{C}$.

$$\begin{aligned}&= \{z : z \in \mathbb{C}, |z|/|2| = 1\} \\ &= \{z : z \in \mathbb{C}, |z| = 2\}\end{aligned}$$

☁ We can write ‘ $\{z : z \in \mathbb{C}, \dots\}$ ’ more simply as ‘ $\{z \in \mathbb{C} : \dots\}$ ’. ☁

$$= \{z \in \mathbb{C} : |z| = 2\}.$$

This is the circle with centre 0 and radius 2 in the complex plane.

Similarly,

$$\begin{aligned} 3i \operatorname{Ker} \phi &= \{3iz : z \in \operatorname{Ker} \phi\} \\ &= \{3iz : z \in \mathbb{C}, |z| = 1\} \\ &= \{z : z/(3i) \in \mathbb{C}, |z/(3i)| = 1\} \\ &= \{z : z \in \mathbb{C}, |z|/|3i| = 1\} \\ &= \{z \in \mathbb{C} : |z| = 3\}. \end{aligned}$$

This is the circle with centre 0 and radius 3 in the complex plane.

(b) For any $a \in \mathbb{C}^*$,

$$\begin{aligned} a \operatorname{Ker} \phi &= \{az : z \in \operatorname{Ker} \phi\} \\ &= \{az : z \in \mathbb{C}, |z| = 1\} \\ &= \{z : z/a \in \mathbb{C}, |z/a| = 1\} \\ &= \{z : z \in \mathbb{C}, |z|/|a| = 1\} \\ &= \{z \in \mathbb{C} : |z| = |a|\}. \end{aligned}$$

This is the circle with centre 0 and radius $|a|$ in the complex plane.

(c) The elements of the quotient group $\mathbb{C}^*/\operatorname{Ker} \phi$ are the sets of the form

$$\{z \in \mathbb{C} : |z| = r\}$$

where $r \in \mathbb{R}^+$.

That is, they are the circles with centre 0 and positive radius in the complex plane (the complex number 0 itself is not one of these circles). (Some of these circles are shown in Figure 30.)

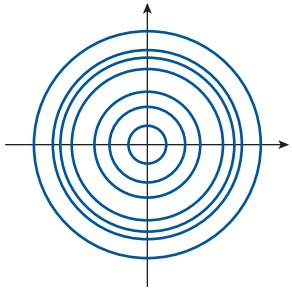


Figure 30 Circles with centre 0 in the complex plane

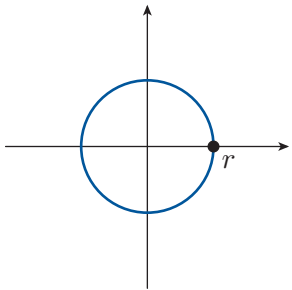


Figure 31 The circle with centre 0 and radius r contains the complex number r

We can describe the binary operation of the quotient group in Worked Exercise E54 in terms of the circles that are its elements. The circle with centre 0 and positive radius r is the coset of $\operatorname{Ker} \phi$ containing the number r (which is an element of \mathbb{C}^* , as shown in Figure 31), so it can be denoted by

$$r \operatorname{Ker} \phi.$$

The rule for set composition of such cosets is (by Theorem E1 in Unit E2)

$$r \operatorname{Ker} \phi \cdot s \operatorname{Ker} \phi = (rs) \operatorname{Ker} \phi,$$

where $r, s \in \mathbb{R}^+$. That is, the binary operation of the quotient group $\mathbb{C}^*/\operatorname{Ker} \phi$ has the rule

$$(\text{circle of radius } r) \cdot (\text{circle of radius } s) = (\text{circle of radius } rs),$$

for all $r, s \in \mathbb{R}^+$.

So the quotient group $\mathbb{C}^*/\text{Ker } \phi$ in Worked Exercise E54 is the group of all circles with centre 0 and positive radius in the complex plane under this binary operation.

The elements of this group and the definition of its binary operation appear to indicate that it is isomorphic to the group (\mathbb{R}^+, \times) , and indeed this is what was found using the First Isomorphism Theorem in the solution to Worked Exercise E51 in the previous subsection.

Exercise E133

Consider the homomorphism

$$\begin{aligned}\phi : (\mathbb{R}^2, +) &\longrightarrow (\mathbb{R}, +) \\ (x, y) &\longmapsto x + y.\end{aligned}$$

You saw that this mapping is a homomorphism in Exercise E129 in Subsection 3.2. You also saw there that its kernel is

$$\text{Ker } \phi = \{(x, y) \in \mathbb{R}^2 : y = -x\}.$$

This is the line $y = -x$ in \mathbb{R}^2 , that is, the line through the origin with gradient -1 .

(Alternatively we can write $\text{Ker } \phi$ as

$$\text{Ker } \phi = \{(k, -k) : k \in \mathbb{R}\}.)$$

- Find the particular coset $(2, 3) + \text{Ker } \phi$ and describe it geometrically.
- Find the general coset $(a, b) + \text{Ker } \phi$, where $(a, b) \in \mathbb{R}^2$, and describe it geometrically.
- Hence specify the elements of the quotient group $\mathbb{R}^2/\text{Ker } \phi$ and describe them geometrically.

As for the quotient group in Worked Exercise E54, we can describe the binary operation of the quotient group in Exercise E133 in terms of the geometric interpretation of its elements. You should have found that the elements of the quotient group $\mathbb{R}^2/\text{Ker } \phi$ in Exercise E133 are the lines in the plane with gradient -1 .

The rule for set composition of these elements is (by Theorem E1 in Unit E2)

$$((0, c) + \text{Ker } \phi) + ((0, d) + \text{Ker } \phi) = ((0, c) + (0, d)) + \text{Ker } \phi,$$

that is,

$$((0, c) + \text{Ker } \phi) + ((0, d) + \text{Ker } \phi) = (0, c + d) + \text{Ker } \phi.$$

We can express this rule as

$$(\text{line } y = -x + c) + (\text{line } y = -x + d) = (\text{line } y = -x + (c + d)).$$

So the quotient group $\mathbb{R}^2/\text{Ker } \phi$ in Exercise E133 is the group of lines in the plane with gradient -1 under this binary operation.

The elements of this group and the definition of its binary operation appear to indicate that it is isomorphic to the group $(\mathbb{R}, +)$, and indeed this is what was found using the First Isomorphism Theorem in the solution to Exercise E129 in the previous subsection.

Summary

In this unit you have met the idea of a *homomorphism* from a group to a group, and considered many examples. You have seen that homomorphisms preserve important features of the structure of the domain group, including composites, the identity, inverses, powers and conjugates. You have studied the *image* and *kernel* of a homomorphism, and explored some of the properties of these sets, such as the fact that they are always groups themselves. You have also learned that kernels of homomorphisms and normal subgroups are in fact the same objects. You have seen that a linear transformation is a special type of homomorphism, and met several parallels between homomorphisms in group theory and linear transformations in linear algebra. Finally you met the *First Isomorphism Theorem*, which links homomorphisms and quotient groups.

Learning outcomes

After working through this unit, you should be able to:

- explain what is meant by a *homomorphism*
- understand that an isomorphism is a special case of a homomorphism
- check whether a mapping between groups is a homomorphism, or an isomorphism, or neither
- understand that a homomorphism preserves composites, the identity, inverses, powers, conjugates and the properties of being abelian and being cyclic
- understand what are meant by the *image* and *kernel* of a homomorphism
- understand that the image of a homomorphism is a subgroup of the codomain group, and the kernel of a homomorphism is a normal subgroup of the domain group
- know that a homomorphism is one-to-one if and only if its kernel contains the identity element of the domain group alone
- understand that all the elements in a coset of the kernel of a homomorphism have the same image under the homomorphism
- understand that, for any homomorphism, the quotient group formed by the cosets of the kernel is isomorphic to the image group (the *First Isomorphism Theorem*).

Solutions to exercises

Solution to Exercise E99

(a) As mentioned in the question, the given group tables (repeated here for convenience) have the same pattern:

| \circ | e | a | r | s | \times_{12} | 1 | 5 | 7 | 11 |
|---------|-----|-----|-----|-----|---------------|----|----|----|----|
| e | e | a | r | s | 1 | 1 | 5 | 7 | 11 |
| a | a | e | s | r | 5 | 5 | 1 | 11 | 7 |
| r | r | s | e | a | 7 | 7 | 11 | 1 | 5 |
| s | s | r | a | e | 11 | 11 | 7 | 5 | 1 |

$(S(\square), \circ)$
 (U_{12}, \times_{12})

So the following mapping ϕ_1 , obtained by matching up the row (or column) labels in order, is an isomorphism.

$$\begin{aligned}\phi_1 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 1 \\ a &\longmapsto 5 \\ r &\longmapsto 7 \\ s &\longmapsto 11\end{aligned}$$

Now consider the following mappings ϕ_2 and ϕ_3 .

$$\begin{aligned}\phi_2 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 1 \\ a &\longmapsto 5 \\ r &\longmapsto 11 \\ s &\longmapsto 7\end{aligned}$$

$$\begin{aligned}\phi_3 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 1 \\ a &\longmapsto 7 \\ r &\longmapsto 5 \\ s &\longmapsto 11\end{aligned}$$

Replacing each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_2 and its image under ϕ_3 , respectively, gives the following tables.

| | 1 | 5 | 11 | 7 | | 1 | 7 | 5 | 11 |
|----|----|----|----|----|----|----|----|----|----|
| 1 | 1 | 5 | 11 | 7 | 1 | 1 | 7 | 5 | 11 |
| 5 | 5 | 1 | 7 | 11 | 7 | 7 | 1 | 11 | 5 |
| 11 | 11 | 7 | 1 | 5 | 5 | 5 | 11 | 1 | 7 |
| 7 | 7 | 11 | 5 | 1 | 11 | 11 | 5 | 7 | 1 |

Each of these tables is a correct group table for (U_{12}, \times_{12}) (because, for each table, each cell in the body of the table contains the result of combining the row label of the cell with the column label of the cell). So both ϕ_2 and ϕ_3 are isomorphisms.

(In fact there are six different isomorphisms from $(S(\square), \circ)$ to (U_{12}, \times_{12}) : any one-to-one and onto mapping from $(S(\square), \circ)$ to (U_{12}, \times_{12}) that maps the identity element e of $(S(\square), \circ)$ to the identity element 1 of (U_{12}, \times_{12}) is an isomorphism.)

(b) Consider the following one-to-one and onto mapping ϕ_4 from $(S(\square), \circ)$ to (U_{12}, \times_{12}) .

$$\begin{aligned}\phi_4 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 5 \\ a &\longmapsto 1 \\ r &\longmapsto 7 \\ s &\longmapsto 11\end{aligned}$$

Replacing each entry in the group table of $S(\square)$ above by its image under ϕ_4 gives the following table.

| | 5 | 1 | 7 | 11 |
|----|----|----|----|----|
| 5 | 5 | 1 | 7 | 11 |
| 1 | 1 | 5 | 11 | 7 |
| 7 | 7 | 11 | 5 | 1 |
| 11 | 11 | 7 | 1 | 5 |

This is not a group table of (U_{12}, \times_{12}) because, for example, it is not true that $5 \times_{12} 5 = 5$.

Hence ϕ_4 is an example of a one-to-one and onto mapping from $(S(\square), \circ)$ to (U_{12}, \times_{12}) that is not an isomorphism.

(There are other possible answers here: any one-to-one and onto mapping from $(S(\square), \circ)$ to (U_{12}, \times_{12}) that does *not* map e to 1 will do.)

Solution to Exercise E100

The given group table for $(S^+(\square), \circ)$ is as follows. (It is repeated here for convenience.)

| \circ | e | a | b | c |
|---------|-----|-----|-----|-----|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

Consider the following one-to-one and onto mapping from $(S^+(\square), \circ)$ to (U_{10}, \times_{10}) .

$$\begin{aligned}\phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 3 \\ b &\longmapsto 7 \\ c &\longmapsto 9\end{aligned}$$

Replacing each entry in the group table of $(S^+(\square), \circ)$ above by its image under ϕ gives the following table.

| | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 7 | 9 | 1 |
| 7 | 7 | 9 | 1 | 3 |
| 9 | 9 | 1 | 3 | 7 |

This is not a group table of (U_{10}, \times_{10}) because, for example, it is not true that $3 \times_{10} 3 = 7$.

Hence ϕ is an example of a one-to-one and onto mapping from $(S^+(\square), \circ)$ to (U_{10}, \times_{10}) that maps the identity element of $(S^+(\square), \circ)$ to the identity element of (U_{10}, \times_{10}) but is not an isomorphism.

(There are other possible answers here: any one-to-one and onto mapping from $(S^+(\square), \circ)$ to (U_{10}, \times_{10}) that maps e to 1 but does not map b (the only element of order 2 in $(S^+(\square), \circ)$) to 9 (the only element of order 2 in (U_{10}, \times_{10})) will do. There are three such mappings other than the one above, as follows.

$$\begin{aligned}\phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 7 \\ b &\longmapsto 3 \\ c &\longmapsto 9\end{aligned}$$

$$\begin{aligned}\phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 9 \\ b &\longmapsto 3 \\ c &\longmapsto 7\end{aligned}$$

$$\begin{aligned}\phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 9 \\ b &\longmapsto 7 \\ c &\longmapsto 3\end{aligned}$$

Solution to Exercise E101

The group table of $(S(\square), \circ)$ is as follows. (It is repeated here for convenience.)

| \circ | e | a | r | s |
|---------|-----|-----|-----|-----|
| e | e | a | r | s |
| a | a | e | s | r |
| r | r | s | e | a |
| s | s | r | a | e |

The following mapping ϕ_1 maps every element of $(S(\square), \circ)$ to itself, so it is an isomorphism and hence an automorphism.

$$\begin{aligned}\phi_1 : (S(\square), \circ) &\longrightarrow (S(\square), \circ) \\ e &\longmapsto e \\ a &\longmapsto a \\ r &\longmapsto r \\ s &\longmapsto s\end{aligned}$$

Now consider the following mapping ϕ_2 .

$$\begin{aligned}\phi_2 : (S(\square), \circ) &\longrightarrow (S(\square), \circ) \\ e &\longmapsto e \\ a &\longmapsto r \\ r &\longmapsto a \\ s &\longmapsto s\end{aligned}$$

Replacing each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_2 gives the following table.

| | e | r | a | s |
|-----|-----|-----|-----|-----|
| e | e | r | a | s |
| r | r | e | s | a |
| a | a | s | e | r |
| s | s | a | r | e |

This table is a correct group table for $(S(\square), \circ)$, so ϕ_2 is an isomorphism and hence an automorphism.

(There are six different automorphisms of $(S(\square), \circ)$: any one-to-one and onto mapping from $(S(\square), \circ)$ to itself that maps e to itself will do.)

Solution to Exercise E102

The mapping ϕ (the exponential function) is one-to-one.

It is also onto, because its image set is $(0, \infty) = \mathbb{R}^+$.

We now check that ϕ preserves composites. Let $x, y \in \mathbb{R}$. We have to show that

$$\phi(x + y) = \phi(x) \times \phi(y),$$

that is,

$$e^{x+y} = e^x \times e^y.$$

This is true by the index laws for \mathbb{R} , so ϕ preserves composites.

Hence ϕ is an isomorphism.

Solution to Exercise E103

To show that ϕ is one-to-one, suppose that m and n are elements of \mathbb{Z} such that

$$\phi(m) = \phi(n).$$

Then

$$-m = -n,$$

which gives

$$m = n.$$

Thus ϕ is one-to-one.

Also, ϕ is onto, because each element n of the codomain group $(\mathbb{Z}, +)$ is the image under ϕ of the element $-n$ of the domain group $(\mathbb{Z}, +)$.

We now check that ϕ preserves composites. Let $m, n \in \mathbb{Z}$. We have to show that

$$\phi(m + n) = \phi(m) + \phi(n).$$

Now

$$\begin{aligned} \phi(m + n) &= -(m + n) \\ &= (-m) + (-n) \\ &= \phi(m) + \phi(n). \end{aligned}$$

Thus ϕ preserves composites.

Hence ϕ is an isomorphism.

Solution to Exercise E104

(a) This mapping ϕ is not one-to-one. For example, $\phi(i) = \phi(1) = 1$.

(This mapping ϕ is onto and preserves composites.)

(b) This mapping ϕ is not onto. For example, the element 1 of the codomain is not the image under ϕ of any element of the domain.

(This mapping ϕ is one-to-one and preserves composites.)

(c) This mapping ϕ is not onto, because $2^x > 0$ for all $x \in \mathbb{R}$, so, for example, the element -1 of the codomain is not the image under ϕ of any element of the domain.

In fact, this mapping ϕ does not preserve composites either as, in general, $2^{x \times y} \neq 2^x \times 2^y$. For example,

$$\phi(1 \times 2) = 2^{1 \times 2} = 2^2 = 4$$

whereas

$$\phi(1) \times \phi(2) = 2^1 \times 2^2 = 2 \times 4 = 8.$$

(This mapping ϕ is one-to-one.)

Solution to Exercise E105

The group $(\mathbb{Z}_{10}, +_{10})$ is a cyclic group of order 10, generated by 1. In this group the consecutive multiples of the generator 1 starting from the identity 0 are

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \dots$$

We try to find a generator of the group $(\mathbb{Z}_{11}^*, \times_{11})$. In $(\mathbb{Z}_{11}^*, \times_{11})$ the consecutive powers of 2 starting from 2^0 are

$$1, 2, 4, 8, 5, 10, 9, 7, 3, 6, \dots$$

All the elements of \mathbb{Z}_{11}^* appear in this list, so 2 is a generator of $(\mathbb{Z}_{11}^*, \times_{11})$.

Matching each multiple of the generator 1 of $(\mathbb{Z}_{10}, +_{10})$ to the corresponding power of the generator 2 of $(\mathbb{Z}_{11}^*, \times_{11})$ gives the following isomorphism:

$$\begin{aligned} \phi : (\mathbb{Z}_{10}, +_{10}) &\longrightarrow (\mathbb{Z}_{11}^*, \times_{11}) \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 8 \\ 4 &\longmapsto 5 \\ 5 &\longmapsto 10 \\ 6 &\longmapsto 9 \\ 7 &\longmapsto 7 \\ 8 &\longmapsto 3 \\ 9 &\longmapsto 6. \end{aligned}$$

(There are alternative answers, as follows, since 6, 7 and 8 are also generators of $(\mathbb{Z}_{11}^*, \times_{11})$:

| | | |
|--------------------|--------------------|--------------------|
| $0 \longmapsto 1$ | $0 \longmapsto 1$ | $0 \longmapsto 1$ |
| $1 \longmapsto 6$ | $1 \longmapsto 7$ | $1 \longmapsto 8$ |
| $2 \longmapsto 3$ | $2 \longmapsto 5$ | $2 \longmapsto 9$ |
| $3 \longmapsto 7$ | $3 \longmapsto 2$ | $3 \longmapsto 6$ |
| $4 \longmapsto 9$ | $4 \longmapsto 3$ | $4 \longmapsto 4$ |
| $5 \longmapsto 10$ | $5 \longmapsto 10$ | $5 \longmapsto 10$ |
| $6 \longmapsto 5$ | $6 \longmapsto 4$ | $6 \longmapsto 3$ |
| $7 \longmapsto 8$ | $7 \longmapsto 6$ | $7 \longmapsto 2$ |
| $8 \longmapsto 4$ | $8 \longmapsto 9$ | $8 \longmapsto 5$ |
| $9 \longmapsto 2$ | $9 \longmapsto 8$ | $9 \longmapsto 7.$ |

Solution to Exercise E106

In the group $(\mathbb{Z}_4, +_4)$ the consecutive multiples of the generator 1 starting from the identity 0 are

$$0, 1, 2, 3, \dots$$

In the group $(\mathbb{Z}_8, +_8)$ the consecutive multiples of 2 starting from the identity 0 are

$$0, 2, 4, 6, \dots$$

Thus the cyclic subgroup of $(\mathbb{Z}_8, +_8)$ generated by 2 is $\langle 2 \rangle = \{0, 2, 4, 6\}$.

Matching each multiple of the generator 1 of $(\mathbb{Z}_4, +_4)$ to the corresponding multiple of the generator 2 of the subgroup $\langle 2 \rangle$ of $(\mathbb{Z}_8, +_8)$ gives the following isomorphism:

$$\begin{aligned} \phi : (\mathbb{Z}_4, +_4) &\longrightarrow (\{0, 2, 4, 6\}, +_4) \\ 0 &\longmapsto 0 \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 6. \end{aligned}$$

(The subgroup of $(\mathbb{Z}_8, +_8)$ generated by 2 is also generated by 6, so an alternative answer is

$$\begin{aligned} \phi : (\mathbb{Z}_4, +_4) &\longrightarrow (\{0, 2, 4, 6\}, +_4) \\ 0 &\longmapsto 0 \\ 1 &\longmapsto 6 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 2. \end{aligned}$$

Solution to Exercise E107

(a) The homomorphism property for ϕ is

$$\phi(x \times y) = \phi(x) \times \phi(y) \quad \text{for all } x, y \in \mathbb{R}^*.$$

We check whether it holds. Let $x, y \in \mathbb{R}^*$. Then

$$\begin{aligned} \phi(x \times y) &= (x \times y)^2 \\ &= x^2 \times y^2 \\ &= \phi(x) \times \phi(y). \end{aligned}$$

Thus ϕ is a homomorphism.

(b) The homomorphism property for ϕ is

$$\phi(m + n) = \phi(m) + \phi(n) \quad \text{for all } m, n \in \mathbb{Z}.$$

The mapping ϕ does not have this property, since, for example, $1 \in \mathbb{Z}$ and

$$\phi(1 + 1) = \phi(2) = 2^2 = 4,$$

whereas

$$\phi(1) + \phi(1) = 1^2 + 1^2 = 1 + 1 = 2,$$

so $\phi(1+1) \neq \phi(1) + \phi(1)$. Hence ϕ is not a homomorphism.

(c) The homomorphism property for ϕ is

$$\phi(m +_6 n) = \phi(m) +_6 \phi(n) \quad \text{for all } m, n \in \mathbb{Z}_6.$$

We check whether it holds. Let $m, n \in \mathbb{Z}_6$. Then

$$\begin{aligned} \phi(m +_6 n) &= 3 \times_6 (m +_6 n) \\ &= (3 \times_6 m) +_6 (3 \times_6 n) \\ &\text{(by the distributive law for modular arithmetic)} \\ &= \phi(m) +_6 \phi(n). \end{aligned}$$

Thus ϕ is a homomorphism.

(d) The homomorphism property for ϕ is

$$\phi(m + n) = \phi(m) \times \phi(n) \quad \text{for all } m, n \in \mathbb{Z}.$$

We check whether it holds. Let $m, n \in \mathbb{Z}$. Then

$$\begin{aligned} \phi(m + n) &= 2^{m+n} \\ &= 2^m \times 2^n \\ &= \phi(m) \times \phi(n). \end{aligned}$$

Thus ϕ is a homomorphism.

(e) The homomorphism property for ϕ is

$$\phi(x + y) = \phi(x) +_2 \phi(y) \quad \text{for all } x, y \in \mathbb{R}.$$

The mapping ϕ does not have this property, since, for example, $\pi \in \mathbb{R}$ and

$$\phi(\pi + \pi) = \phi(2\pi) = 1$$

whereas

$$\phi(\pi) +_2 \phi(\pi) = 1 +_2 1 = 0.$$

So $\phi(\pi + \pi) \neq \phi(\pi) +_2 \phi(\pi)$. Hence ϕ is not a homomorphism.

(The number 2π is irrational, because if 2π were rational then $\pi = (2\pi)/2$ would be rational.)

(f) The homomorphism property for ϕ is

$$\begin{aligned} \phi((x_1, y_1) + (x_2, y_2)) &= \phi(x_1, y_1) + \phi(x_2, y_2) \\ &\text{for all } (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2. \end{aligned}$$

We check whether it holds. Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$.

The left-hand side of the homomorphism property equation is

$$\begin{aligned} &\phi((x_1, y_1) + (x_2, y_2)) \\ &= \phi(x_1 + x_2, y_1 + y_2) \\ &= (2(x_1 + x_2) - (y_1 + y_2), 6(x_1 + x_2) - 3(y_1 + y_2)) \\ &= (2x_1 + 2x_2 - y_1 - y_2, 6x_1 + 6x_2 - 3y_1 - 3y_2). \end{aligned}$$

The right-hand side is

$$\begin{aligned} &\phi(x_1, y_1) + \phi(x_2, y_2) \\ &= (2x_1 - y_1, 6x_1 - 3y_1) + (2x_2 - y_2, 6x_2 - 3y_2) \\ &= (2x_1 + 2x_2 - y_1 - y_2, 6x_1 + 6x_2 - 3y_1 - 3y_2). \end{aligned}$$

Since the two sides are equal, ϕ is a homomorphism.

(In fact, as you will see later in this subsection, there is a shortcut way to confirm that this mapping is a homomorphism, using the fact that it is a linear transformation from the vector space \mathbb{R}^2 to itself.)

(For simplicity, we write $\phi(x, y)$ for $\phi((x, y))$, as in Unit C3 *Linear transformations*.)

Solution to Exercise E108

Let $f, g \in S_n$. We have to show that

$$\phi(f \circ g) = \phi(f) +_2 \phi(g).$$

We know that a composite of two even permutations or two odd permutations is even, and a composite of a even permutation and an odd permutation is odd. Thus we have the following.

If f is even and g is even then $f \circ g$ is even so

$$\phi(f \circ g) = 0 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 0 +_2 0 = 0.$$

If f is even and g is odd then $f \circ g$ is odd so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 0 +_2 1 = 1.$$

If f is odd and g is even then $f \circ g$ is odd so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 1 +_2 0 = 1.$$

If f is odd and g is odd then $f \circ g$ is even so

$$\phi(f \circ g) = 0 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 1 +_2 1 = 0.$$

Thus in all cases $\phi(f \circ g) = \phi(f) +_2 \phi(g)$. Hence ϕ is a homomorphism.

Solution to Exercise E109

(a) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$.

Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ 0 & uy \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix} \begin{pmatrix} v & 0 \\ 0 & y \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ 0 & uy \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(b) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$.

Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ rv - uy & uy \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \begin{pmatrix} r & 0 \\ r - u & u \end{pmatrix} \begin{pmatrix} v & 0 \\ v - y & y \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ rv - uv + uv - uy & uy \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ rv - uy & uy \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

Solution to Exercise E110

The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in \text{GL}(2).$$

The mapping ϕ does not have this property. For example, the matrices

$$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

are both elements of $\text{GL}(2)$ (since they both have determinant 1 and are therefore invertible), and

$$\begin{aligned} \phi(\mathbf{AB}) &= (\mathbf{AB})^{-1} \\ &= \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right)^{-1} \\ &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \end{aligned}$$

whereas

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \mathbf{A}^{-1}\mathbf{B}^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) \neq \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is not a homomorphism.

Solution to Exercise E111

(a) The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A}) + \phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in L.$$

The mapping ϕ does not have this property. For example, the matrix

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is an element of L , and

$$\phi(\mathbf{II}) = \phi(\mathbf{I}) = 1 + 1 = 2,$$

whereas

$$\phi(\mathbf{I}) + \phi(\mathbf{I}) = 1 + 1 + 1 + 1 = 4.$$

Thus $\phi(\mathbf{II}) \neq \phi(\mathbf{I}) + \phi(\mathbf{I})$. Hence ϕ is not a homomorphism.

(b) The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in L.$$

We check whether it holds. Let $\mathbf{A}, \mathbf{B} \in L$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\left(\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix}\right) \\ &= (rv)^2(uy)^2 \\ &= (ruvy)^2 \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\right)\phi\left(\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= r^2u^2v^2y^2 \\ &= (ruvy)^2. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(c) The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in L.$$

We check whether it holds. Let $\mathbf{A}, \mathbf{B} \in L$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$.

Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\left(\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix}\right) \\ &= \frac{rv}{uy} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\right)\phi\left(\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \frac{r}{u} \times \frac{v}{y} \\ &= \frac{rv}{uy}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

Solution to Exercise E112

First we prove the ‘if’ part. Suppose that G is abelian. Then, for all $x, y \in G$,

$$\begin{aligned} \phi(x \circ y) &= (x \circ y) \circ (x \circ y) \\ &= x \circ (y \circ x) \circ y \\ &= x \circ (x \circ y) \circ y \quad (\text{since } G \text{ is abelian}) \\ &= (x \circ x) \circ (y \circ y) \\ &= \phi(x) \circ \phi(y). \end{aligned}$$

Hence ϕ is a homomorphism.

Now we prove the ‘only if’ part. Suppose that ϕ is a homomorphism. Then, for all $x, y \in G$,

$$\phi(x \circ y) = \phi(x) \circ \phi(y),$$

that is,

$$(x \circ y) \circ (x \circ y) = (x \circ x) \circ (y \circ y).$$

We can write this as

$$x \circ (y \circ x) \circ y = x \circ (x \circ y) \circ y.$$

It now follows by the Cancellation Laws that

$$y \circ x = x \circ y.$$

Hence G is abelian.

Thus ϕ is a homomorphism if and only if G is abelian.

Solution to Exercise E113

Let $x, y, z \in G$. Then

$$\begin{aligned}\phi(x \circ y \circ z) &= \phi((x \circ y) \circ z) \\ &= \phi(x \circ y) * \phi(z) \\ &\quad (\text{by the homomorphism property for } \phi) \\ &= (\phi(x) * \phi(y)) * \phi(z) \\ &\quad (\text{by the homomorphism property for } \phi \text{ again}) \\ &= \phi(x) * \phi(y) * \phi(z),\end{aligned}$$

as required.

Solution to Exercise E114

(a) The identity in both the domain group and the codomain group is 1, and $\phi(1) = 1^2 = 1$.

(b) The identity in both the domain group and the codomain group is 0, and $\phi(0) = 3 \times_6 0 = 0$.

Solution to Exercise E115

(a) In \mathbb{R}^* , the inverse of 3 is $\frac{1}{3}$. Now

$$\phi(3) = 9 \quad \text{and} \quad \phi\left(\frac{1}{3}\right) = \frac{1}{9}.$$

In \mathbb{R}^* , the elements 9 and $\frac{1}{9}$ are inverses of each other.

(b) In \mathbb{Z}_6 , the inverse of 4 is 2. Now

$$\phi(4) = 0 \quad \text{and} \quad \phi(2) = 0.$$

In \mathbb{Z}_6 , the element 0 is the inverse of 0.

Solution to Exercise E116

(a) In \mathbb{R}^* ,

$$\phi(3^2) = \phi(9) = 9^2 = 81$$

and

$$(\phi(3))^2 = 9^2 = 81,$$

so $\phi(3^2) = (\phi(3))^2$.

(b) In \mathbb{Z}_6 ,

$$\phi(4 +_6 4) = \phi(2) = 3 \times_6 2 = 0$$

and

$$\begin{aligned}\phi(4) +_6 \phi(4) &= (3 \times_6 4) +_6 (3 \times_6 4) \\ &= 0 +_6 0 = 0,\end{aligned}$$

so $\phi(4 +_6 4) = \phi(4) +_6 \phi(4)$.

Solution to Exercise E117

(a) The image of ϕ_3 is $\{1, 3, 5, 7\} = U_8$, its whole codomain.

(b) The image of ϕ_4 is \mathbb{R}^+ , again its whole codomain.

Solution to Exercise E118

(a) The homomorphism ϕ maps each integer n to its remainder on division by 12.

It is not one-to-one because, for example, $\phi(1) = \phi(13)$.

However, each element of \mathbb{Z}_{12} occurs as an image under ϕ , so $\text{Im } \phi = \mathbb{Z}_{12}$ and hence ϕ is onto.

(b) The homomorphism ϕ is one-to-one, because if $m, n \in \mathbb{Z}$ and $\phi(m) = \phi(n)$, then $2^m = 2^n$, which gives $m = n$.

The image of ϕ is the set of all integer powers of 2. That is,

$$\text{Im } \phi = \{2^n : n \in \mathbb{Z}\}.$$

There is no integer n such that $2^n = 3$, for example, so ϕ is not onto.

Solution to Exercise E119

(a) The group $(\mathbb{Z}_{12}, +_{12})$ is cyclic so, by Theorem E49, any homomorphism with this group as its domain group must have a cyclic image. This image cannot be $(S(\triangle), \circ)$, because this group is not cyclic.

Alternatively, you may have observed that \mathbb{Z}_{12} is abelian, but $(S(\triangle), \circ)$ is not.

(b) The first argument given in part (a) applies to this case too, because $(S(\square), \circ)$ is not cyclic.

(However, $(S(\square), \circ)$ is abelian, so the second argument does not apply here.)

Solution to Exercise E120

(a) The identity element of the codomain group of ϕ_3 is 1. The kernel of ϕ_3 is $\{e\}$.

(b) The identity element of the codomain group of ϕ_4 is 1. The kernel of ϕ_4 is $\{1, -1\}$.

Solution to Exercise E121

(a) The elements of \mathbb{Z}_6 are 0, 1, 2, 3, 4 and 5, and 0 is the identity element. We have

$$\begin{aligned}\phi(0) &= 0, \\ \phi(1) &= 3, \\ \phi(2) &= 0, \\ \phi(3) &= 3, \\ \phi(4) &= 0, \\ \phi(5) &= 3.\end{aligned}$$

Hence $\text{Im } \phi = \{0, 3\}$ and $\text{Ker } \phi = \{0, 2, 4\}$.

(b) This homomorphism ϕ , the exponential function, has image $(0, \infty) = \mathbb{R}^+$ (as you saw in Subsection 4.2 of Unit D4). That is,

$$\text{Im } \phi = \mathbb{R}^+.$$

(So ϕ is onto.)

Also, ϕ is one-to-one (since it is strictly increasing, as you saw in Subsection 4.2 of Unit D4). Hence, since the identity element in the domain group is 0,

$$\text{Ker } \phi = \{0\},$$

by Theorem E52.

(c) This is the trivial homomorphism from (\mathbb{R}^*, \times) to (\mathbb{R}^*, \times) . Every element of the domain group is mapped by ϕ to the identity element 1 of the codomain group. Therefore

$$\text{Im } \phi = \{1\}$$

and $\text{Ker } \phi$ is the whole domain group, that is,

$$\text{Ker } \phi = \mathbb{R}^*.$$

Solution to Exercise E122

First we show that ϕ is a homomorphism. Let $m, n \in \mathbb{Z}$. We have to show that

$$\phi(m+n) = \phi(m) + \phi(n).$$

Now

$$\begin{aligned}\phi(m+n) &= 7(m+n) \\ &= 7m + 7n \\ &= \phi(m) + \phi(n).\end{aligned}$$

Hence ϕ is a homomorphism.

Now we find the image of ϕ . It is

$$\begin{aligned}\text{Im } \phi &= \{\phi(n) : n \in \mathbb{Z}\} \\ &= \{7n : n \in \mathbb{Z}\} \\ &= 7\mathbb{Z} \\ &= \{\dots, -14, -7, 0, 7, 14, \dots\}.\end{aligned}$$

(The final line above could be omitted.)

Finally we find the kernel of ϕ . The identity element of the codomain group is 0. So the kernel is

$$\begin{aligned}\text{Ker } \phi &= \{n \in \mathbb{Z} : \phi(n) = 0\} \\ &= \{n \in \mathbb{Z} : 7n = 0\} \\ &= \{n \in \mathbb{Z} : n = 0\} \\ &= \{0\}.\end{aligned}$$

(Alternatively, we can find the kernel by showing that ϕ is one-to-one and applying Theorem E52.)

Solution to Exercise E123

We have

$$\begin{aligned}\text{Im } \phi &= \left\{ \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix} : d \in \mathbb{R}, d \neq 0 \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} : r \in \mathbb{R}^+ \right\}.\end{aligned}$$

(Here we have used the fact that, as d runs through all non-zero values in \mathbb{R} , its square d^2 takes all *positive* values in \mathbb{R} , so we can specify the set $\text{Im } \phi$ equally well by replacing d^2 with r , say, where $r \in \mathbb{R}^+$.)

The identity element of the codomain group (L, \times) is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so

$$\text{Ker } \phi = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Now

$$\begin{aligned}\phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\iff \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &\iff d^2 = 1 \\ &\iff d = \pm 1.\end{aligned}$$

Thus

$$\begin{aligned}\text{Ker } \phi &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : d = \pm 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0, d = \pm 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & \pm 1 \end{pmatrix} : a, c \in \mathbb{R}, a \neq 0 \right\}.\end{aligned}$$

Solution to Exercise E124

The identity element of the codomain group (D, \times)

is the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so

$$\begin{aligned}\text{Ker } \phi &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : a = d = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0, a = d = 1 \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} : c \in \mathbb{R} \right\}.\end{aligned}$$

Solution to Exercise E125

Let r be an element of the codomain group (\mathbb{R}^*, \times) . Then the matrix

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$$

is an element of the domain group (L, \times) , because it is lower triangular and its determinant is $r \times 1 = r$ which is non-zero because $r \in \mathbb{R}^*$, and

$$\phi \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} = r.$$

Thus ϕ is onto and therefore $\text{Im } \phi = \mathbb{R}^*$.

Solution to Exercise E126

First we show that $\text{Im } \phi \subseteq \mathbb{R}^+$. Let $r \in \text{Im } \phi$. Then

$$r = \phi(x)$$

for some element x of \mathbb{R}^* . This gives

$$r = x^2.$$

Since $x \in \mathbb{R}^*$, it follows that $r > 0$ and hence $r \in \mathbb{R}^+$. Therefore $\text{Im } \phi \subseteq \mathbb{R}^+$.

Now we show that $\mathbb{R}^+ \subseteq \text{Im } \phi$. Let $r \in \mathbb{R}^+$. Then r is the image under ϕ of the real number \sqrt{r} , since

$$\phi(\sqrt{r}) = (\sqrt{r})^2 = r.$$

Hence $r \in \text{Im } \phi$. Therefore $\mathbb{R}^+ \subseteq \text{Im } \phi$.

Since $\text{Im } \phi \subseteq \mathbb{R}^+$ and $\mathbb{R}^+ \subseteq \text{Im } \phi$, it follows that $\text{Im } \phi = \mathbb{R}^+$.

Solution to Exercise E127

(a) The mapping ϕ is a homomorphism because, for any $m, n \in \mathbb{Z}_{12}$,

$$\begin{aligned}\phi(m +_{12} n) &= 2 \times_{12} (m +_{12} n) \\ &= (2 \times_{12} m) +_{12} (2 \times_{12} n) \\ &= \phi(m) +_{12} \phi(n).\end{aligned}$$

(b) The identity element of the codomain group is 0, so

$$\begin{aligned}\text{Ker } \phi &= \{n \in \mathbb{Z}_{12} : \phi(n) = 0\} \\ &= \{n \in \mathbb{Z}_{12} : 2 \times_{12} n = 0\} \\ &= \{0, 6\}.\end{aligned}$$

The cosets of $\text{Ker } \phi$ are

$$\begin{aligned}\text{Ker } \phi &= \{0, 6\}, \\ 1 + \text{Ker } \phi &= \{1, 7\}, \\ 2 + \text{Ker } \phi &= \{2, 8\}, \\ 3 + \text{Ker } \phi &= \{3, 9\}, \\ 4 + \text{Ker } \phi &= \{4, 10\}, \\ 5 + \text{Ker } \phi &= \{5, 11\}.\end{aligned}$$

(c) We have

$$\begin{aligned}\phi(0) &= \phi(6) = 0, \\ \phi(1) &= \phi(7) = 2, \\ \phi(2) &= \phi(8) = 4, \\ \phi(3) &= \phi(9) = 6, \\ \phi(4) &= \phi(10) = 8, \\ \phi(5) &= \phi(11) = 10.\end{aligned}$$

Thus the partition of \mathbb{Z}_{12} obtained by collecting together elements of \mathbb{Z}_{12} with the same image is

$$\{0, 6\}, \quad \{1, 7\}, \quad \{2, 8\}, \quad \{3, 9\}, \quad \{4, 10\}, \quad \{5, 11\}.$$

As expected this is the same as the partition of \mathbb{Z}_{12} into cosets of $\text{Ker } \phi$ found in part (b).

Solution to Exercise E128

(a) The kernel of ϕ is the set of integers that ϕ maps to 0, so

$$\text{Ker } \phi = \{5n : n \in \mathbb{Z}\} = 5\mathbb{Z}.$$

The cosets of $\text{Ker } \phi$ are

$$\begin{aligned} 5\mathbb{Z} &= \{5n : n \in \mathbb{Z}\}, \\ 1 + 5\mathbb{Z} &= \{5n + 1 : n \in \mathbb{Z}\}, \\ 2 + 5\mathbb{Z} &= \{5n + 2 : n \in \mathbb{Z}\}, \\ 3 + 5\mathbb{Z} &= \{5n + 3 : n \in \mathbb{Z}\}, \\ 4 + 5\mathbb{Z} &= \{5n + 4 : n \in \mathbb{Z}\}. \end{aligned}$$

(b) The set of integers with a particular image, say s , under ϕ is the set of integers whose remainder on division by 5 is s . Thus the partition obtained by collecting together integers with the same image consists of the five sets listed in part (a), as expected.

Solution to Exercise E129

(a) The mapping ϕ is a linear transformation, because it is of the form

$$(x, y) \mapsto ax + by$$

where $a, b \in \mathbb{R}$. Hence, by Proposition E39, it is a homomorphism.

(Alternatively, we can show that ϕ is a homomorphism as follows.

Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. We have to show that

$$\phi((x_1, y_1) + (x_2, y_2)) = \phi(x_1, y_1) + \phi(x_2, y_2).$$

Now

$$\begin{aligned} \phi((x_1, y_1) + (x_2, y_2)) &= \phi(x_1 + x_2, y_1 + y_2) \\ &= (x_1 + x_2) + (y_1 + y_2) \\ &= (x_1 + y_1) + (x_2 + y_2) \\ &= \phi(x_1, y_1) + \phi(x_2, y_2). \end{aligned}$$

Hence ϕ is a homomorphism.)

(b) The homomorphism ϕ is onto, since if x is an element of the codomain group $(\mathbb{R}, +)$ then x is the image under ϕ of the element $(x, 0)$ of the domain group $(\mathbb{R}^2, +)$, because

$$\phi(x, 0) = x + 0 = x.$$

Hence

$$\text{Im } \phi = \mathbb{R}.$$

Also

$$\begin{aligned} \text{Ker } \phi &= \{(x, y) \in \mathbb{R}^2 : \phi(x, y) = 0\} \\ &= \{(x, y) \in \mathbb{R}^2 : x + y = 0\} \\ &= \{(x, y) \in \mathbb{R}^2 : y = -x\}. \end{aligned}$$

(This is the line $y = -x$ in \mathbb{R}^2 , that is, the line through the origin with gradient -1 .)

(Alternatively we can write $\text{Ker } \phi$ as

$$\text{Ker } \phi = \{(k, -k) : k \in \mathbb{R}\}.)$$

(c) By the First Isomorphism Theorem,

$$\mathbb{R}^2 / \text{Ker } \phi \cong \text{Im } \phi,$$

so

$$\mathbb{R}^2 / \text{Ker } \phi \cong (\mathbb{R}, +).$$

So a standard group isomorphic to $\mathbb{R}^2 / \text{Ker } \phi$ is $(\mathbb{R}, +)$.

Solution to Exercise E130

(a) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$, where $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= rvuy \\ &= ruvy \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= ruvy. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(b) The homomorphism ϕ is onto, because if $r \in \mathbb{R}^*$ then r is the image under ϕ of the matrix

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}.$$

This matrix is in L because it is lower triangular and its determinant is $r \times 1 = r$, which is non-zero because $r \in \mathbb{R}^*$. Hence

$$\text{Im } \phi = \mathbb{R}^*.$$

The identity element of the codomain group is 1, so

$$\begin{aligned} \text{Ker } \phi &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : ad = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : d = 1/a \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & 1/a \end{pmatrix} : a, c \in \mathbb{R}, a \neq 0 \right\}. \end{aligned}$$

(c) By the First Isomorphism Theorem,

$$L / \text{Ker } \phi \cong (\mathbb{R}^*, \times).$$

So a standard group isomorphic to $L / \text{Ker } \phi$ is (\mathbb{R}^*, \times) .

Solution to Exercise E131

(a) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi \left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \right) \\ &= \phi \begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \begin{pmatrix} 1/(rv) & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \phi \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \begin{pmatrix} 1/r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/v & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1/(rv) & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(b) We have

$$\begin{aligned} \text{Im } \phi &= \left\{ \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L \right\} \\ &= \left\{ \begin{pmatrix} 1/a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^* \right\} \\ &= \left\{ \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} : r \in \mathbb{R}^* \right\}. \end{aligned}$$

The identity element of the codomain group is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

so

$$\begin{aligned} \text{Ker } \phi &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \begin{pmatrix} 1/a & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : 1/a = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : a = 1 \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} : c, d \in \mathbb{R}, d \neq 0 \right\}. \end{aligned}$$

(c) By the First Isomorphism Theorem, the quotient group $L / \text{Ker } \phi$ is isomorphic to $\text{Im } \phi$.

We now show that $\text{Im } \phi$ is isomorphic to (\mathbb{R}^*, \times) . Consider the mapping

$$\begin{aligned} \theta : \text{Im } \phi &\longrightarrow \mathbb{R}^* \\ \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} &\longmapsto r. \end{aligned}$$

This mapping is one-to-one, because if

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}$$

are elements of $\text{Im } \phi$ such that $\theta(\mathbf{A}) = \theta(\mathbf{B})$, then $r = s$ by the definition of θ and hence $\mathbf{A} = \mathbf{B}$.

It is also onto, because if $r \in \mathbb{R}^*$ then r is the image under θ of the element

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$$

of $\text{Im } \phi$.

Finally, it has the homomorphism property because, for all $r, s \in \mathbb{R}^*$,

$$\begin{aligned} \theta \left(\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} \right) &= \theta \begin{pmatrix} rs & 0 \\ 0 & 1 \end{pmatrix} \\ &= rs \\ &= \theta \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \theta \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Thus θ is an isomorphism, so

$$L / \text{Ker } \phi \cong \text{Im } \phi \cong (\mathbb{R}^*, \times).$$

Solution to Exercise E132

(a) Let $\phi : \mathbb{Z}_{11} \rightarrow S_3$ be a homomorphism. By Corollary E56 and Lagrange's Theorem, the order of $\text{Im } \phi$ divides the orders of \mathbb{Z}_{11} and S_3 , which are 11 and 6, respectively. But 11 and 6 have greatest common factor 1, so the order of $\text{Im } \phi$ is 1. Hence, since $\text{Im } \phi$ is a subgroup of S_3 , we have $\text{Im } \phi = \{e\}$. Therefore ϕ is the trivial homomorphism

$$\begin{aligned} \phi : \mathbb{Z}_{11} &\rightarrow S_3 \\ n &\mapsto e. \end{aligned}$$

(b) Let $\phi : S(\triangle) \rightarrow \mathbb{Z}_3$ be a homomorphism. By Corollary E56 and Lagrange's Theorem, the order of $\text{Im } \phi$ divides the orders of $S(\triangle)$ and \mathbb{Z}_3 , which are 6 and 3, respectively. Hence the order of $\text{Im } \phi$ is either 1 or 3.

If $\text{Im } \phi$ has order 3, then $\text{Ker } \phi$ has order 2, by Corollary E56. As $S(\triangle)$ does not have a normal subgroup of order 2 (by the solution to Exercise E39 in Subsection 3.3 of Unit E2), this is impossible.

Thus $\text{Im } \phi$ has order 1. Hence, since $\text{Im } \phi$ is a subgroup of $(\mathbb{Z}_3, +_3)$, we have $\text{Im } \phi = \{0\}$. Therefore ϕ is the trivial homomorphism

$$\begin{aligned} \phi : S(\triangle) &\rightarrow \mathbb{Z}_3 \\ f &\mapsto 0. \end{aligned}$$

Solution to Exercise E133

(a) We have

$$\begin{aligned} (2, 3) + \text{Ker } \phi &= \{(2 + x, 3 + y) : (x, y) \in \mathbb{R}^2, y = -x\} \\ &= \{(x, y) : (x - 2, y - 3) \in \mathbb{R}^2, y - 3 = -(x - 2)\} \\ &= \{(x, y) : (x, y) \in \mathbb{R}^2, y = -x + 5\} \\ &= \{(x, y) \in \mathbb{R}^2 : y = -x + 5\}. \end{aligned}$$

This is the line $y = -x + 5$, that is, the line with gradient -1 and y -intercept 5.

(Alternatively we can find $(2, 3) + \text{Ker } \phi$ as follows.

$$\begin{aligned} (2, 3) + \text{Ker } \phi &= \{(2 + k, 3 - k) : k \in \mathbb{R}\} \\ &= \{(k, 3 - (k - 2)) : k - 2 \in \mathbb{R}\} \\ &= \{(k, -k + 5) : k \in \mathbb{R}\}. \end{aligned}$$

This is the line $y = -x + 5$.)

(A third way to find the coset $(2, 3) + \text{Ker } \phi$ is as follows. Since $\text{Ker } \phi$ is the line $y = -x$, the coset $(2, 3) + \text{Ker } \phi$ is the line obtained by translating the line $y = -x$ by two units to the right and three units up. Since the line $y = -x$ has gradient -1 , translating it by two units to the right increases its y -intercept by 2 units, and then translating it by three units up increases its y -intercept by another 3 units. Its gradient remains unchanged throughout, so we obtain the line $y = -x + 5$.)

(b) Similarly,

$$\begin{aligned} (a, b) + \text{Ker } \phi &= \{(a + x, b + y) : (x, y) \in \mathbb{R}^2, y = -x\} \\ &= \{(x, y) : (x - a, y - b) \in \mathbb{R}^2, y - b = -(x - a)\} \\ &= \{(x, y) : (x, y) \in \mathbb{R}^2, y = -x + (a + b)\} \\ &= \{(x, y) \in \mathbb{R}^2 : y = -x + (a + b)\}. \end{aligned}$$

This is the line $y = -x + (a + b)$, that is, the line with gradient -1 and y -intercept $a + b$.

(Alternatively we can find $(a, b) + \text{Ker } \phi$ as follows.

$$\begin{aligned}(a, b) + \text{Ker } \phi &= \{(a + k, b - k) : k \in \mathbb{R}\} \\ &= \{(k, b - (k - a)) : k - a \in \mathbb{R}\} \\ &= \{(k, -k + (a + b)) : k \in \mathbb{R}\}.\end{aligned}$$

This is the line $y = -x + (a + b)$.)

(A third way to find the coset $(a, b) + \text{Ker } \phi$ is as follows. Since $\text{Ker } \phi$ is the line $y = -x$, the coset $(a, b) + \text{Ker } \phi$ is the line obtained by translating the line $y = -x$ by a units to the right and b units up (if a is negative then the translation by a units to the right is actually a translation to the left, and similarly if b is negative then the translation by b units up is actually a translation down). Since the line $y = -x$ has gradient -1 , translating it by a units to the right adds a units to its y -intercept, and then translating it by b units up adds another b units to its y -intercept. Its gradient remains unchanged throughout, so we obtain the line $y = -x + (a + b)$.)

(c) By part (b), each coset of $\text{Ker } \phi$ is a line of the form

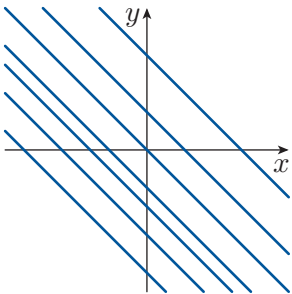
$$y = -x + c,$$

where $c \in \mathbb{R}$. Moreover, each such line is a coset of $\text{Ker } \phi$ because, for any $c \in \mathbb{R}$, the line $y = -x + c$ is the coset

$$(0, c) + \text{Ker } \phi.$$

Thus the elements of the quotient group $\mathbb{R}^2 / \text{Ker } \phi$ are the lines with gradient -1 .

(Some of these elements are shown below.)



Unit E4

Group actions

Introduction

In this unit you will explore the idea that the elements of a group can ‘act’ on the elements of a set. You have already met some instances in which this happens: for example, the elements of a symmetric group S_n act on the elements of the set $\{1, 2, \dots, n\}$. You will see that studying this idea can lead to new insights, both about groups and about the sets on which they act.

You will meet many examples of such ‘group actions’ in this unit, and study some properties that they all share. You will see how the idea of a group action can help to unify some of the theory covered in the earlier group theory units. Later in the unit you will learn how we can use group actions to help us solve counting problems that involve symmetry, such as the following: How many different cubes are there with each face painted blue, yellow or red, if two such cubes are regarded as the same when one can be rotated to give the other?

1 Group actions

In this first section you will learn what is meant by a group action, and meet a variety of examples.

It can take a while to develop a good intuitive understanding of what a group action is, so do not be concerned if you still feel uncertain about this after working through the first subsection, which includes the definition. The many examples in the subsections that follow will help to clarify the idea.

1.1 What is a group action?

Throughout the group theory units you have met many groups *whose elements are functions from a set to itself* and whose binary operation is function composition. Here are two examples.

- The symmetric group S_3 . Each element of S_3 is a permutation of the set $\{1, 2, 3\}$ and so is a function from the set $\{1, 2, 3\}$ to itself.
- The symmetry group $S(\square)$. Each element of $S(\square)$ is a rotation or reflection of the plane \mathbb{R}^2 that maps the square to itself and so is a function from the set \mathbb{R}^2 to itself.

In mathematics there are many instances where we have a group (G, \circ) and a set X , as illustrated in Figure 1, and the elements of G ‘map’ the elements of X to elements of the same set in some way. There may be such a mapping effect even if the elements of G are *not actually functions with domain X* . Here are four examples, starting with a familiar one.

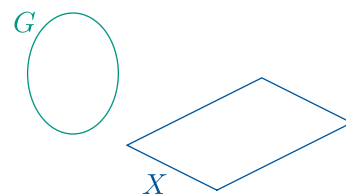
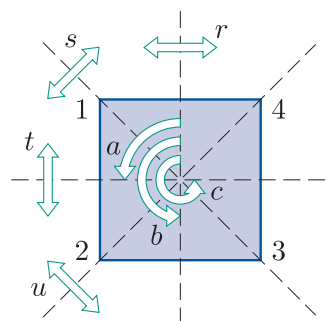
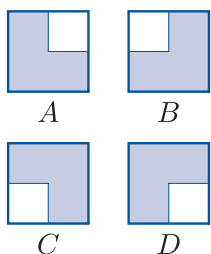


Figure 1 A group (G, \circ) and a set X

**Figure 2** $S(\square)$ **Figure 3** Four modified squares

1. The group $S(\square) = \{e, a, b, c, r, s, t, u\}$ and the set $\{1, 2, 3, 4\}$ of vertex labels of the square, as shown in Figure 2. Each element of $S(\square)$ maps the elements of $\{1, 2, 3, 4\}$ to elements of the same set.
2. The group $S(\square) = \{e, a, b, c, r, s, t, u\}$ and the set $\{A, B, C, D\}$ of modified squares shown in Figure 3. Each element of $S(\square)$ maps the elements of $\{A, B, C, D\}$ to elements of the same set, in the obvious way. For example, the element a of $S(\square)$ maps A to B .
3. The group $\text{GL}(2)$ of all invertible 2×2 matrices with real entries, and the set V , say, of all 2-dimensional column vectors with real entries. One way in which each matrix in $\text{GL}(2)$ can map the vectors in V to vectors in V is by matrix multiplication. For example, the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ maps the vector $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$ to the vector $\begin{pmatrix} 3 \\ -2 \end{pmatrix}$.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}.$$
4. The group $(\mathbb{Z}, +)$ and the set \mathbb{R} of real numbers. One way in which each element of $(\mathbb{Z}, +)$ can map the elements of \mathbb{R} to elements of \mathbb{R} is by addition. For example, the element 3 of $(\mathbb{Z}, +)$ adds 3 to each element of \mathbb{R} , so it maps 1 to 4, and 0.5 to 3.5, and so on.

In each of these examples there is a ‘mapping effect’ of the group on the stated set, even though the elements of the group are not functions whose domain is the stated set. In examples 3 and 4 the elements of the group are not functions at all. In examples 1 and 2 the elements of the group *are* functions, but the domain of these functions is not the stated set.

Throughout this unit we will be studying mapping effects like these of groups on sets. Before we can make a start, we need to define a notation that we can use for such mapping effects. When a group element g ‘maps’ a set element x to another set element, we will not usually denote the ‘image’ of x ‘under’ g by $g(x)$, as you might expect. Instead, we will use the notation

$$g \wedge x,$$

which is read as ‘ g wedge x ’. This notation is more convenient in some situations. However, it has the disadvantage that it is less intuitive.

Whenever you see it, you might find it helpful to think of it as essentially meaning ‘ $g(x)$ ’. The group element g is behaving like a function whose domain contains the set element x .

As an example of the notation, consider the effect of the group $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 4). The element a of $S(\square)$ maps vertex 2 to vertex 3, so we write

$$a \wedge 2 = 3.$$

Here is an exercise to help you get used to this notation.

Exercise E134

- (a) Consider the effect of the group $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square, as shown in Figure 4. Write down the following.
 - (i) $r \wedge 2$ (ii) $b \wedge 1$
- (b) Consider the effect of the group $S(\square)$ on the set $\{A, B, C, D\}$ of modified squares shown in Figure 5. Write down the following.
 - (i) $b \wedge B$ (ii) $s \wedge B$
- (c) Consider the effect of the symmetric group S_3 on the set $\{1, 2, 3\}$ of symbols. Write down the following.
 - (i) $(1\ 3\ 2) \wedge 2$ (ii) $(1\ 2) \wedge 3$
- (d) Consider the effect of the group $GL(2)$ of all invertible 2×2 matrices with real entries on the set V of all 2-dimensional column vectors with real entries, by matrix multiplication. Write down the following.
 - (i) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \wedge \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ (ii) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \wedge \begin{pmatrix} -1 \\ 4 \end{pmatrix}$
- (e) Consider the effect of the group $(\mathbb{Z}, +)$ on the set \mathbb{R} of real numbers by addition. Write down the following.
 - (i) $3 \wedge 7.4$ (ii) $1 \wedge -0.3$

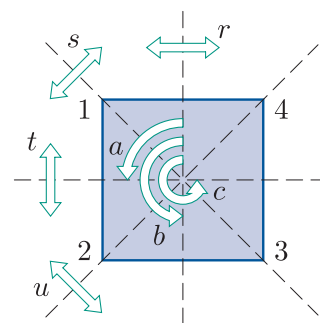


Figure 4 $S(\square)$

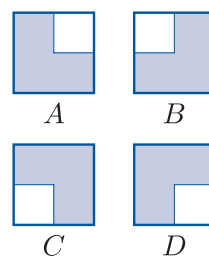


Figure 5 Four modified squares

The $g \wedge x$ notation introduced above will be used throughout this unit. Unfortunately, this is just one of several notations used by mathematicians for the ‘image’ of a set element x ‘under’ a group element g – there is no standard notation. The alternative notations that you might see in other texts include $g \cdot x$, $g * x$, x^g and simply gx .

We will not be interested in *all* mapping effects of groups on sets. Mathematicians have found that the ones that are useful and interesting are those that have three key properties. These properties are as follows, where (G, \circ) is a group that has a mapping effect on a set X .

- The first property is simply that the elements of G must ‘map’ the elements of X to elements of the same set X , rather than mapping them to objects that are outside X . That is, for each g in G and each x in X we must have

$$g \wedge x \in X.$$

This is illustrated in Figure 6.

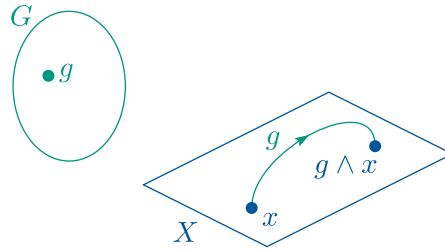


Figure 6 The group element g must ‘map’ each element of the set X to an element of the set X

- The second property is that the identity element e of (G, \circ) must behave as the *identity function* on X . Recall that the **identity function** on a set X is the function from X to X that **fixes** each element of X , that is, maps each element of X to itself. So, for each x in X we must have

$$e \wedge x = x.$$

This is illustrated in Figure 7.

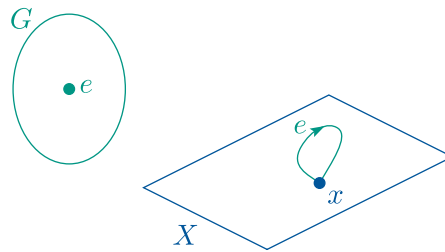


Figure 7 The identity element e of (G, \circ) must ‘map’ each element x of the set X to itself

- The third property is that the binary operation \circ of the group (G, \circ) must behave like function composition. If the elements of the group (G, \circ) were *actually* functions with domain X and the binary operation \circ were *actually* function composition, then the following equation would be true for all g and h in G and all x in X :

$$g(h(x)) = (g \circ h)(x).$$

This is just the definition of function composition. So, translating into the $g \wedge x$ notation, we require the binary operation \circ of G to satisfy the following equation for all g and h in G and all x in X :

$$g \wedge (h \wedge x) = (g \circ h) \wedge x.$$

In other words, it must be the case that if g and h are any elements of the group (G, \circ) and x is any element of the set X , then applying h to x and then applying g to the result gives the same answer as applying $g \circ h$ to x . This is illustrated in Figure 8.

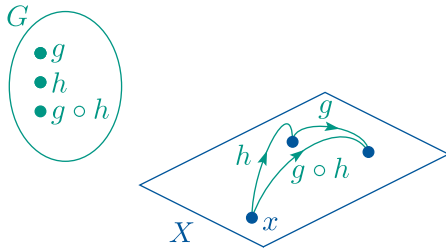


Figure 8 Applying h and then g to x must give the same result as applying $g \circ h$ to x

If a mapping effect of a group (G, \circ) on a set X does have the three properties above, then we say that it is a *group action*, and that (G, \circ) *acts on* X . You will see later in this section that examples 1–4 of mapping effects of groups on sets that were given earlier in this subsection are all group actions.

The definition of a group action is summarised below. Note that the group (G, \circ) and the set X of a group action can each be either finite or infinite.

Definition

Let (G, \circ) be a group with identity element e , and let X be a set. Suppose that for each element g in G and each element x in X an object $g \wedge x$ is defined in some way.

We say that the effect \wedge of (G, \circ) on X is a **group action** of (G, \circ) on X , or simply an **action** of (G, \circ) on X , and that (G, \circ) **acts on** X , if the following three axioms hold.

GA1 Closure For each $g \in G$ and each $x \in X$,

$$g \wedge x \in X.$$

GA2 Identity For each $x \in X$,

$$e \wedge x = x.$$

GA3 Composition For all $g, h \in G$ and all $x \in X$,

$$g \wedge (h \wedge x) = (g \circ h) \wedge x.$$

We call the three axioms in this definition the **group action axioms**.

The next worked exercise demonstrates how to check the group action axioms. In this example, the group is a group of functions, the set on which the group has a mapping effect is the domain of these functions, and \wedge is defined to be simply the usual mapping effect of the functions on the elements of the set, that is, $g \wedge x = g(x)$. (This is in fact the first example of a group of functions given right at the start of this subsection.)



Worked Exercise E55

Consider the symmetric group S_3 and the set $\{1, 2, 3\}$ of symbols. Let \wedge be defined by

$$g \wedge x = g(x)$$

for all $g \in S_3$ and all $x \in \{1, 2, 3\}$. Show that \wedge is a group action.

Solution

 We apply the definition of a group action. Here the group (G, \circ) is (S_3, \circ) and the set X is the set $\{1, 2, 3\}$ of symbols. 

We check the group action axioms.

GA1 Closure

 We have to show that for each $g \in S_3$ and each $x \in \{1, 2, 3\}$,

$$g \wedge x \in \{1, 2, 3\}. \quad \text{img alt="pencil icon" data-bbox="525 490 548 510"}$$

Let $g \in S_3$ and let $x \in \{1, 2, 3\}$. Then, since g is a permutation of $\{1, 2, 3\}$,

$$g \wedge x = g(x) \in \{1, 2, 3\}.$$

Thus axiom GA1 holds.

GA2 Identity

 We have to show that for each $x \in \{1, 2, 3\}$,

$$e \wedge x = x,$$

where e is the identity element of S_3 . 

The identity element e of S_3 is the identity permutation of $\{1, 2, 3\}$. So for each $x \in \{1, 2, 3\}$, we have

$$e \wedge x = e(x) = x.$$

Thus axiom GA2 holds.

GA3 Composition

 We have to show that for all $g, h \in S_3$ and all $x \in \{1, 2, 3\}$,

$$g \wedge (h \wedge x) = (g \circ h) \wedge x. \quad \text{cloud icon}$$

Let $g, h \in S_3$ and let $x \in \{1, 2, 3\}$. Then

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge (h(x)) && \text{(by the definition of } \wedge) \\ &= g(h(x)) && \text{(by the definition of } \wedge) \\ &= (g \circ h)(x) && \\ &&& \text{(by the definition of function composition)} \\ &= (g \circ h) \wedge x && \text{(by the definition of } \wedge). \end{aligned}$$

Thus axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

The reason why axiom GA3 holds in Worked Exercise E55 is, in essence, that when \wedge is defined to be the normal mapping effect of a group of functions on the domain of the functions, the statement of axiom GA3 is just the definition of function composition.

You can practise checking the group action axioms in the next exercise.

The group involved is the subgroup of the symmetric group S_5 whose elements are all the permutations in S_5 that either fix the symbols 4 and 5 or transpose them. For example, these permutations include $(1\ 2\ 3)$, which fixes 4 and 5, and $(1\ 2\ 3)(4\ 5)$, which transposes 4 and 5. These permutations *do* form a subgroup of S_5 , by the result of Exercise E17(a) in Subsection 1.4 of Unit E1 *Cosets and normal subgroups*. You were asked to list the elements of this subgroup in part (b) of that exercise.

Exercise E135

Let G be the subgroup of the symmetric group S_5 that consists of all the permutations in S_5 that either fix the symbols 4 and 5 or transpose them.

Consider this group G and the set $X = \{1, 2, 3\}$. (The set X is a subset of the set $\{1, 2, 3, 4, 5\}$ of symbols permuted by the elements of S_5 .) Let \wedge be defined by

$$g \wedge x = g(x)$$

for all $g \in G$ and all $x \in X$. Show that \wedge is a group action.

The next exercise asks you to show that two mapping effects of groups on sets are *not* group actions. Remember that to do this you need only show that *one* of the group action axioms does not hold, by giving a counterexample.

Exercise E136

Show that neither of the following is a group action.

- (a) The mapping effect \wedge of the symmetric group S_5 on the set $\{1, 2, 3\}$ of symbols defined by

$$g \wedge x = g(x)$$

for all $g \in S_5$ and all $x \in \{1, 2, 3\}$.

- (b) The mapping effect \wedge of the group (\mathbb{R}^*, \times) on the set \mathbb{R}^2 of points in the plane defined by

$$g \wedge (x, y) = (x + g, y + g)$$

for all $g \in \mathbb{R}^*$ and all $(x, y) \in \mathbb{R}^2$.

Now consider again the group action in Exercise E135. The group G here is the group of all permutations in S_5 that fix or transpose the symbols 4 and 5, the set X is the set $\{1, 2, 3\}$ of symbols, and the mapping effect \wedge is given by

$$g \wedge x = g(x)$$

for all $g \in G$ and all $x \in X$. (The exercise asked you to show that this *is* a group action.)

This example illustrates an important point about group actions. When a group G acts on a set X , it is possible for two or more different elements of G to have exactly the same mapping effect on the elements of X . That is, two or more different elements of G can ‘behave as the same function’ from X to X .

For example, for the group action in Exercise E135 the permutations $(1\ 2\ 3)$ and $(1\ 2\ 3)(4\ 5)$ are both elements of the group G , and they both have the same effect on the elements of the set $X = \{1, 2, 3\}$: each of them maps 1 to 2, 2 to 3 and 3 to 1. Similarly, the elements $(1\ 2)$ and $(1\ 2)(4\ 5)$ of G both have the same effect on X , and the elements e and $(4\ 5)$ of G both have the same effect on X , and so on. In fact, for this group action it is possible to pair off the elements of the group G in such a way that the two elements in each pair have the same effect on the set X . (The two elements in each pair are permutations of the form g and $g \circ (4\ 5)$.)

In contrast, for the group action in Worked Exercise E55, which is the usual mapping effect of the symmetric group S_3 on the set $S = \{1, 2, 3\}$ of symbols, all the elements of the group S_3 have *different* effects on the elements of the set S . That is, each group element ‘behaves as a different function’.

An action of a group G on a set X in which no two elements of G behave as the same function from X to X is called a **faithful** group action. So the group action in Exercise E135 is not faithful, whereas that in Worked Exercise E55 is faithful.

We now turn to a fundamental property of group actions. To help us describe this property concisely, it is useful to introduce the following definition that applies to functions.

Definition

A one-to-one and onto function from a set X to itself is called a **permutation** of X . (The set X may be either finite or infinite.)

We say that such a function **permutes** the elements of X .

This definition is a generalisation of the similar definition for permutations of *finite* sets, which you met in Subsection 1.1 of Unit B3 *Permutations*. Informally, no matter whether a set is finite or infinite, a permutation of the set is a function that ‘shuffles’ the elements of the set. For example, reflections and rotations of the plane \mathbb{R}^2 are permutations of \mathbb{R}^2 .

In each of the group actions in Worked Exercise E55 and Exercise E135, the mapping effect of each group element on the set involved in the action is that of a one-to-one and onto function from the set to itself. In other words, each group element behaves as a *permutation* of this set. The theorem below tells us that this is always the case for a group action. Part (a) of the theorem states that the effect of each group element on the set is one-to-one, and part (b) states that it is onto.

Theorem E57

Let \wedge be an action of a group G on a set X . Then \wedge has the following properties.

- (a) For each g in G , if x and y are elements of X such that $g \wedge x = g \wedge y$, then $x = y$.
- (b) For each g in G , if y is an element of X then there is an element x of X such that $g \wedge x = y$.

Proof

- (a) Let g be an element of G and suppose that x and y are elements of X such that $g \wedge x = g \wedge y$. By axiom GA1 the object $g \wedge x$, equal to $g \wedge y$, is an element of X , so $g^{-1} \wedge (g \wedge x)$ and $g^{-1} \wedge (g \wedge y)$ exist and

$$g^{-1} \wedge (g \wedge x) = g^{-1} \wedge (g \wedge y).$$

Hence, by axiom GA3,

$$(g^{-1} \circ g) \wedge x = (g^{-1} \circ g) \wedge y;$$

that is,

$$e \wedge x = e \wedge y.$$

By axiom GA2, this gives

$$x = y,$$

as required.

- (b) Let g be an element of G , and let y be an element of X . By axiom GA2,

$$e \wedge y = y,$$

which we can write as

$$(g \circ g^{-1}) \wedge y = y.$$

By axiom GA3, this gives

$$g \wedge (g^{-1} \wedge y) = y.$$

Now $g^{-1} \wedge y$ is an element of X by axiom GA1, so if we take $x = g^{-1} \wedge y$ then $x \in X$ and $g \wedge x = y$, as required. ■

So, by what you have seen in this subsection, we can say the following.

When a group G acts on a set X , we can think of each element of G as behaving like a permutation of the set X , but we have to remember that two or more elements of G may behave like the same permutation.

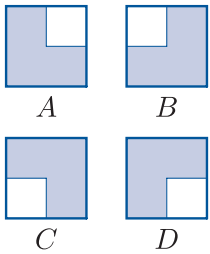


Figure 9 Four modified squares

Often in this unit we will be dealing with a group G that has an *obvious* mapping effect on a set X . For example, the group S_3 has an obvious mapping effect on the set $\{1, 2, 3\}$ of symbols, and the group $S(\square)$ has an obvious mapping effect on the set of modified squares shown in Figure 9, as mentioned earlier. If such a mapping effect is a group action, then we refer to this group action as the **natural action** of G on X , or simply **the action** of G on X . We also say that G **acts on X in the natural way**. So where you see a reference to an action of a group G on a set X with no specification of what the action is, you should assume that it is the natural action of G on X . (It is usually possible to define other, less obvious, group actions of the same group G on the same set X .)

We end this subsection with a result that provides many examples of group actions. You saw in Worked Exercise E55 that the usual mapping effect of the group S_3 on the set $\{1, 2, 3\}$ of symbols is a group action. The following more general result holds. Its proof is a straightforward generalisation of the solution to Worked Exercise E55.

Proposition E58

For any natural number n , the usual mapping effect of the group S_n or any of its subgroups on the set $\{1, 2, \dots, n\}$ of symbols is a group action.

Proof Let n be a natural number, and let (G, \circ) be a subgroup of S_n . The usual mapping effect \wedge of the group (G, \circ) on the set $\{1, 2, \dots, n\}$ is given by $g \wedge x = g(x)$ for all $g \in G$ and all $x \in \{1, 2, \dots, n\}$. We check the group action axioms for this mapping effect.

GA1 Closure

Let $g \in G$ and let $x \in \{1, 2, \dots, n\}$. Then, since g is a permutation of $\{1, 2, \dots, n\}$,

$$g \wedge x = g(x) \in \{1, 2, \dots, n\}.$$

Thus axiom GA1 holds.

GA2 Identity

The identity element e of G is the identity permutation of $\{1, 2, \dots, n\}$. So for each $x \in \{1, 2, \dots, n\}$, we have

$$e \wedge x = e(x) = x.$$

Thus axiom GA2 holds.

GA3 Composition

Let $g, h \in G$ and let $x \in \{1, 2, \dots, n\}$. Then

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge (h(x)) \quad (\text{by the definition of } \wedge) \\ &= g(h(x)) \quad (\text{by the definition of } \wedge) \\ &= (g \circ h)(x) \\ &\quad (\text{by the definition of function composition}) \\ &= (g \circ h) \wedge x \quad (\text{by the definition of } \wedge). \end{aligned}$$

Thus axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action. ■

Proposition E58 can be generalised still further, to cover groups whose elements are permutations of an *infinite* set, but we will not need this more general result in this unit.

1.2 Actions of groups of symmetries

In this subsection we will look at some examples of group actions in which the group that is acting is the symmetry group of a figure F or one of its subgroups. We call such a group a **group of symmetries** of the figure F .

In most of the examples, the set on which the group acts is a set of figures in \mathbb{R}^2 or \mathbb{R}^3 .

To illustrate the ideas, consider the symmetry group $S(\square)$ (see Figure 10) and the set $\{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8\}$ of modified squares shown in Figure 11. These modified squares are figures in \mathbb{R}^2 : a figure in \mathbb{R}^2 is defined to be a subset of \mathbb{R}^2 , and each modified square consists of all the points in \mathbb{R}^2 that lie on a line or in a shaded area.

Each element of $S(\square)$ has a mapping effect on the eight modified squares, in the obvious way. For example, the element b of $S(\square)$ maps A_1 to A_3 .

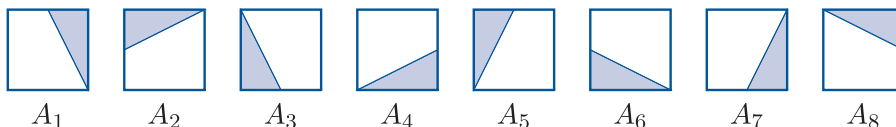


Figure 11 Eight modified squares

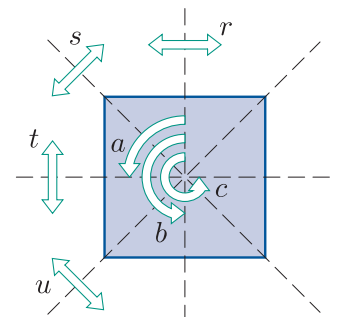


Figure 10 $S(\square)$

This mapping effect of $S(\square)$ on the eight modified squares is a group action, as you will see shortly. To check this, we do not in fact need to check all three group action axioms: we can use Theorem E59 below, which tells us that we need only check axiom GA1, because the other two axioms hold automatically.

The statement of the theorem uses the notation $g(A)$, where A is a figure and g is a transformation, such as a symmetry. This notation means the *image* of A under g , which is given by

$$g(A) = \{g(P) : P \in A\}.$$

In other words, $g(A)$ is the figure obtained by taking the image $g(P)$ of each point P in the figure A under the transformation g . For example, for the figures A_1 and A_3 in Figure 11 (shown again in Figure 12) and the transformation b in $S(\square)$ we have $b(A_1) = A_3$ and $b(A_3) = A_1$.



Figure 12 Two modified squares

Theorem E59

Let G be a group of symmetries of a figure F in \mathbb{R}^2 , and let X be a set of figures in \mathbb{R}^2 . Let \wedge be defined by

$$g \wedge A = g(A),$$

for all $g \in G$ and all $A \in X$. Then \wedge is a group action if and only if axiom GA1 (closure) holds.

The same is true if \mathbb{R}^2 is replaced by \mathbb{R}^3 .

Proof To prove the theorem, we have to check that axioms GA2 and GA3 automatically hold in the situation described.

GA2 Identity

Let e be the identity element of G , and let A be a figure in the set X . We have to show that $e \wedge A = A$.

Now e must be the identity transformation. This is because the elements of G are symmetries not only of the figure F but also of the whole plane \mathbb{R}^2 (or whole space \mathbb{R}^3 , as appropriate), so G is a subgroup of the symmetry group of the whole plane \mathbb{R}^2 (or space \mathbb{R}^3), whose identity element is the identity transformation. Therefore

$$e(P) = P$$

for all points P (in \mathbb{R}^2 or \mathbb{R}^3 as appropriate). Hence

$$e(A) = A;$$

that is,

$$e \wedge A = A.$$

Thus axiom GA2 holds.

GA3 Composition

Let $g, h \in G$ and let A be a figure in the set X . We have to show that

$$g \wedge (h \wedge A) = (g \circ h) \wedge A.$$

By the definition of \wedge , this statement is equivalent to the statement

$$g(h(A)) = (g \circ h)(A).$$

Now, by the definition of function composition, for each point P in the figure A ,

$$g(h(P)) = (g \circ h)(P).$$

Hence

$$g(h(A)) = (g \circ h)(A),$$

as required.

Thus axiom GA3 holds.

This completes the proof. ■

The next worked exercise illustrates how to apply Theorem E59.

In the worked exercise, and throughout this unit, you should assume that if an illustrated figure *appears* to have a certain geometric property, then it *does* have that property. For example, in the worked exercise you should assume that each shaded triangle has a vertex that is the midpoint of an edge of the square.

Worked Exercise E56

In each of parts (a) and (b) below, let X be the set of modified squares shown, and let \wedge be the mapping effect of the group $S(\square)$ (see Figure 13) on the set X given by

$$g \wedge A = g(A)$$

for all $g \in S(\square)$ and all $A \in X$.

In each case, use Theorem E59 to decide whether or not \wedge is a group action. Where it is not a group action, show that it is not.

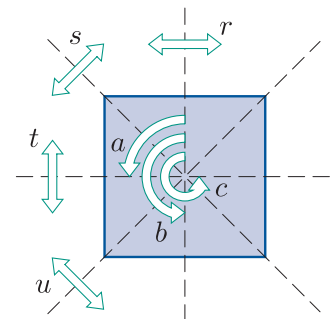
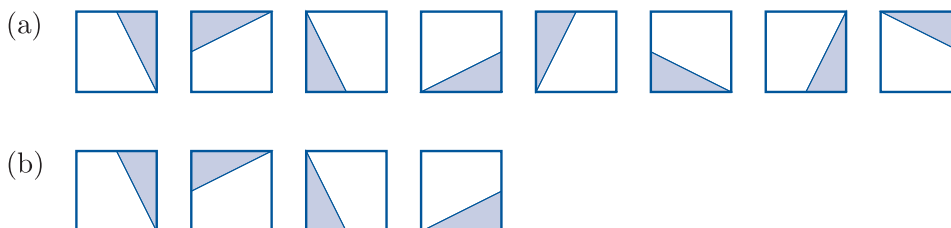


Figure 13 $S(\square)$

Solution

By Theorem E59, in each case \wedge is a group action if and only if axiom GA1 holds, that is, if and only if every element of $S(\square)$ maps each figure in the set X to another figure in X .

- (a) We can see by inspection that every symmetry in $S(\square)$ maps each figure in X to another figure in X . So axiom GA1 holds. Hence, by Theorem E59, \wedge is a group action.
- (b) The element r of $S(\square)$ maps



The first figure here is an element of X but the second figure is not. So axiom GA1 does not hold. Hence, by Theorem E59, \wedge is not a group action.

Worked Exercise E56(a) confirms that the effect of $S(\square)$ on the set of eight modified squares in Figure 11 near the start of this subsection is a group action, as claimed.

Exercise E137

In each of parts (a)–(j) below, let \wedge be the mapping effect of the stated group of symmetries on the given set of figures defined by

$$g \wedge A = g(A)$$

for all symmetries g in the group and all figures A in the set of figures.

In each case use Theorem E59 to decide whether or not \wedge is a group action. Where it is not a group action, show that it is not.

- (a) The group $S(\triangle)$ (see Figure 14) and the set X whose elements are the modified triangles shown below.



- (b) The group $S(\square)$ (see Figure 15) and the set X whose elements are the modified squares shown below.

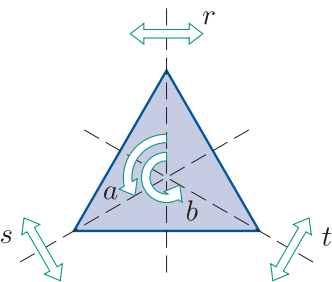
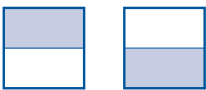


Figure 14 $S(\triangle)$

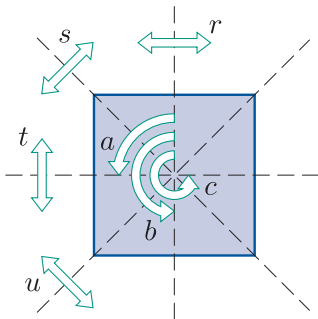


Figure 15 $S(\square)$

- (c) The group $S(\square)$ and the set X whose elements are the modified squares shown below. (These are the modified squares from Figure 3 near the start of the previous subsection.)



- (d) The group $S^+(\square)$ of direct symmetries of the square and the set X whose elements are the modified squares shown below.



- (e) The group $S^+(\square)$ of direct symmetries of the square and the set X whose elements are the modified squares shown below.



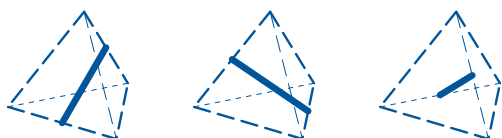
- (f) The group $S(\square)$ and the set whose elements are the four line segments shown below (the lines of symmetry of the square).



- (g) The group $S(\square)$ (see Figure 16) and the set X whose elements are the modified rectangles shown below.



- (h) The group $S(\square)$ of symmetries of the square and the set X of all plane figures.
- (i) The group $S(\text{tet})$ of symmetries of the tetrahedron and the set X whose elements are the three line segments shown below (each line segment joins the midpoints of opposite edges).



- (j) The group $S(\text{tet})$ of symmetries of the tetrahedron and the set X whose elements are the three edges shown below.

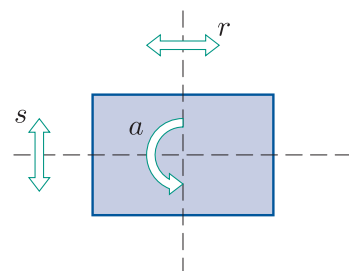
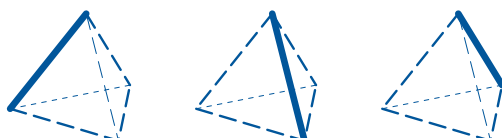


Figure 16 $S(\square)$

We can use Theorem E59 to confirm that the mapping effect of $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square is a group action, as claimed in the previous subsection. Each element of $\{1, 2, 3, 4\}$ is a label for a vertex location of the square, and each vertex location of the square is a figure in \mathbb{R}^2 that consists of a single point. Every element of $S(\square)$ maps each vertex location of the square to another vertex location of the square, so \wedge is a group action by Theorem E59.

You saw in the previous subsection that when a group G acts on a set X each element of G behaves as a *permutation* of the elements of X . The next worked exercise involves writing down such permutations in cycle notation.

Worked Exercise E57

Consider the action of the group $S(\square)$ (see Figure 17) on the set $\{A, B, C, D\}$ whose elements are the modified rectangles shown below.

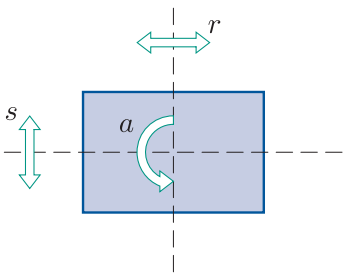
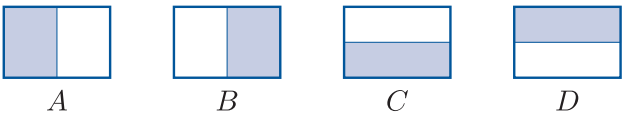


Figure 17 $S(\square)$



(You saw that this is a group action in Exercise E137(g).)

Write down the effect of each element of $S(\square)$ on the set $\{A, B, C, D\}$ as a permutation in cycle form.

Solution

The permutations are as follows. Here we denote the identity permutation of $\{A, B, C, D\}$ by i , since e is used to denote the identity element of $S(\square)$.

| Element g | Permutation |
|-------------|----------------|
| e | i |
| a | $(A\ B)(C\ D)$ |
| r | $(A\ B)$ |
| s | $(C\ D)$ |

Exercise E138

Consider the action of the group $S(\square)$ (see Figure 18) on the set $\{R, S, T, U\}$ of lines of symmetry of the square, as shown below.

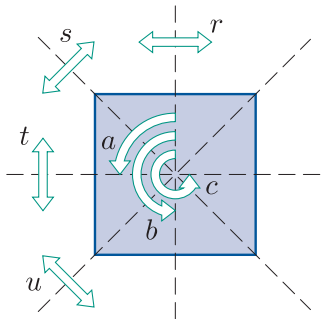


Figure 18 $S(\square)$



(You saw that this is a group action in Exercise E137(f).)

Write down the effect of each element of $S(\square)$ on the set $\{R, S, T, U\}$ as a permutation in cycle form.

Exercise E138 illustrates the fact that, as mentioned in Subsection 1.1, when a group G acts on a set X , two or more elements of G may permute the elements of X in the same way. In other words, a group action may not be *faithful*.

You might have observed more in Exercise E138: the group $S(\square)$ splits into pairs such that the group elements in each pair permute the elements of the set $\{R, S, T, U\}$ in the same way. The same is true for the group action in Exercise E135 in Subsection 1.1, as was mentioned in the subsequent text. In fact, whenever a finite group G acts on a set X , the group G can be partitioned into *subsets of equal size* (not necessarily pairs) such that the group elements in each subset permute the elements of X in the same way. If you would like some insight into why this is, then read the optional short section, Section 5, at the end of this unit.

Actions of symmetry groups on sets of coloured figures

So far we have considered the effects of groups of symmetries only on sets of figures, in either \mathbb{R}^2 or \mathbb{R}^3 . However, as you will see in Section 4, sometimes it is useful to consider the effect of a group of symmetries on a slightly different type of set, namely a set of *coloured* figures. As you would expect, a **coloured figure** is a figure each of whose points has been assigned a colour from a finite set of colours.

For example, consider the group $S(\square)$ (see Figure 19) and the set whose elements are the modified squares shown in Figure 20.

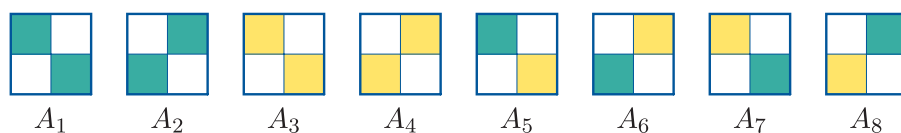


Figure 20 Eight modified squares

Each element of $S(\square)$ has a mapping effect on these eight coloured figures, in the obvious way. For example, the element a of $S(\square)$ maps A_5 to A_6 .

Theorem E59 can be generalised to apply to coloured figures, as well as to ordinary figures. To do this, we need to formally define what we mean by the *image* of a coloured figure under an isometry, such as a symmetry. The definition is just as you would expect, as follows. Suppose that g is an isometry of \mathbb{R}^2 or \mathbb{R}^3 and A is a coloured figure in \mathbb{R}^2 or \mathbb{R}^3 as appropriate. Then the **image** $g(A)$ of A under g consists of the set of points $\{g(P) : P \in A\}$, with each point $g(P)$ in $g(A)$ assigned the same colour as the corresponding point P in A . For example, for the coloured figures in Figure 20, $a(A_5) = A_6$.

Using this definition, we can generalise Theorem E59 as follows.

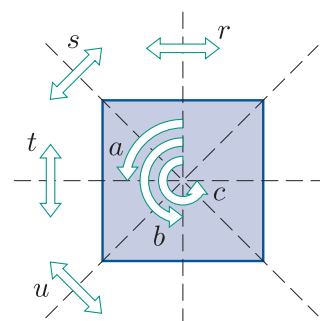


Figure 19 $S(\square)$

Theorem E60

Let G be a group of symmetries of a figure F in \mathbb{R}^2 , and let X be a set of coloured figures in \mathbb{R}^2 . Let \wedge be defined by

$$g \wedge A = g(A),$$

for all $g \in G$ and all $A \in X$. Then \wedge is a group action if and only if axiom GA1 (closure) holds.

The same is true if \mathbb{R}^2 is replaced by \mathbb{R}^3 .

Theorem E60 can be proved in the same way as Theorem E59, except that instead of the proof involving each point P in a figure A , it involves each pair (P, c) where P is a point in the figure A and c is the colour assigned to P . The details are omitted here.

Exercise E139

In each of parts (a), (b) and (c) below, let \wedge be the mapping effect of the stated group of symmetries on the given set of coloured figures defined by

$$g \wedge A = g(A)$$

for all symmetries g in the group and all figures A in the set of figures. In each case use Theorem E60 to decide whether or not \wedge is a group action. Where it is not a group action, show that it is not.

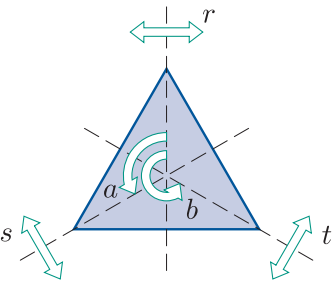


Figure 21 $S(\triangle)$

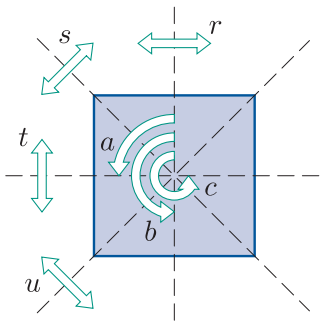
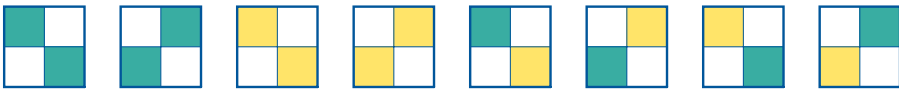


Figure 22 $S(\square)$

- (a) The group $S(\triangle)$ (see Figure 21) and the set X whose elements are the modified triangles shown below.



- (b) The group $S(\square)$ (see Figure 22) and the set X whose elements are the eight modified squares shown below. (These are the modified squares from Figure 20.)



- (c) The group $S(\square)$ and the set X whose elements are all the modified squares obtained by colouring each of the four small squares in the figure below blue, yellow or red.



Some examples of such modified squares are shown below. There are $3^4 = 81$ of them altogether.



Throughout the rest of this unit, we will often work with actions of groups of symmetries on sets of figures or coloured figures. Where you see such an action mentioned, it should be apparent that it *is* a group action by Theorem E59 or Theorem E60. For brevity this is not mentioned every time. (It is mentioned for the first few occurrences.)

1.3 Actions of groups of numbers

In this subsection we will look at some examples of group actions in which the group involved is a group of numbers.

Worked Exercise E58

Consider the group $(\mathbb{Z}, +)$ and the set \mathbb{R} . Let \wedge be defined by

$$g \wedge x = g + x$$

for each $g \in \mathbb{Z}$ and each $x \in \mathbb{R}$. Show that \wedge is a group action.

Solution

We check the group action axioms.

GA1 Closure

We have to show that for each $g \in \mathbb{Z}$ and each $x \in \mathbb{R}$,

$$g \wedge x \in \mathbb{R}. \quad \text{☁}$$

Let $g \in \mathbb{Z}$ and let $x \in \mathbb{R}$. Then

$$g \wedge x = g + x \in \mathbb{R}.$$

Thus axiom GA1 holds.

GA2 Identity

The identity element of the group $(\mathbb{Z}, +)$ is 0.

We have to show that for each $x \in \mathbb{R}$,

$$0 \wedge x = x. \quad \text{☁}$$

Let $x \in \mathbb{R}$. Then

$$0 \wedge x = 0 + x = x.$$

Thus axiom GA2 holds.

GA3 Composition

☁ The binary operation of the group $(\mathbb{Z}, +)$ is $+$, so we have to show that for all $g, h \in \mathbb{Z}$ and all $x \in \mathbb{R}$,

$$g \wedge (h \wedge x) = (g + h) \wedge x. \quad \text{☁}$$

Let $g, h \in \mathbb{Z}$ and let $x \in \mathbb{R}$. We have to show that

$$g \wedge (h \wedge x) = (g + h) \wedge x.$$

Now

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge (h + x) && \text{(by the definition of } \wedge) \\ &= g + (h + x) && \text{(by the definition of } \wedge) \\ &= (g + h) + x \\ &= (g + h) \wedge x && \text{(by the definition of } \wedge). \end{aligned}$$

Thus axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

Exercise E140

Consider the group $(\mathbb{Z}, +)$ and the set \mathbb{R} . Let \wedge be defined by

$$g \wedge x = x - g$$

for each $g \in \mathbb{Z}$ and each $x \in \mathbb{R}$. Show that \wedge is a group action.

Exercise E141

Consider the group $(\mathbb{Z}, +)$ and the set \mathbb{R} . Let \wedge be defined by

$$g \wedge x = g - x$$

for each $g \in \mathbb{Z}$ and each $x \in \mathbb{R}$. Show that \wedge is not a group action.

In the next worked exercise, the group of real numbers under addition acts on the set of points in the plane.

Worked Exercise E59

Consider the group $(\mathbb{R}, +)$ and the set \mathbb{R}^2 . Let \wedge be defined by

$$g \wedge (x, y) = (x + yg, y)$$

for all $g \in \mathbb{R}$ and all $(x, y) \in \mathbb{R}^2$.

Show that \wedge is a group action.

Solution

We check the group action axioms.

GA1 Closure

Let $g \in \mathbb{R}$ and let $(x, y) \in \mathbb{R}^2$. Then

$$g \wedge (x, y) = (x + yg, y) \in \mathbb{R}^2.$$

Thus axiom GA1 holds.

GA2 Identity

The identity element of the group $(\mathbb{R}, +)$ is 0.

Let $(x, y) \in \mathbb{R}^2$. Then

$$0 \wedge (x, y) = (x + y \times 0, y) = (x, y).$$

Thus axiom GA2 holds.

GA3 Composition

Let $g, h \in \mathbb{R}$ and let $(x, y) \in \mathbb{R}^2$.

We have to show that

$$g \wedge (h \wedge (x, y)) = (g + h) \wedge (x, y).$$

Now

$$\begin{aligned} g \wedge (h \wedge (x, y)) &= g \wedge (x + yh, y) \quad (\text{by the definition of } \wedge) \\ &= (x + yh + yg, y) \quad (\text{by the definition of } \wedge) \end{aligned}$$

and

$$\begin{aligned} (g + h) \wedge (x, y) &= (x + (g + h)y, y) \quad (\text{by the definition of } \wedge) \\ &= (x + yh + yg, y). \end{aligned}$$

The two expressions obtained are the same, so axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

In Worked Exercise E59 the equation in axiom GA3 was checked by simplifying each side separately and confirming that the same expression is obtained in each case. This can be a helpful approach when the definition of \wedge is complicated.

Exercise E142

Consider the group $(\mathbb{R}, +)$ and the set \mathbb{R}^2 . Let \wedge be defined by

$$g \wedge (x, y) = (x, y + g)$$

for all $g \in \mathbb{R}$ and all $(x, y) \in \mathbb{R}^2$.

Show that \wedge is a group action.

1.4 Actions of matrix groups

Our final collection of examples of group actions in this section consists of actions of groups of 2×2 matrices on the plane \mathbb{R}^2 .

First consider the group $\text{GL}(2)$ of invertible 2×2 matrices with real entries under matrix multiplication and the set \mathbb{R}^2 of points in the plane. The group $\text{GL}(2)$ has a mapping effect on the set \mathbb{R}^2 given by matrix multiplication on the left, as follows: if

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is an element of $\text{GL}(2)$ and (x, y) is a point in \mathbb{R}^2 , then the matrix \mathbf{A} maps the point (x, y) to the point $(ax + by, cx + dy)$, because

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

This mapping effect is a group action, as stated and proved below.

Theorem E61

Let \wedge be defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \wedge (x, y) = (ax + by, cx + dy)$$

for all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2)$ and all points $(x, y) \in \mathbb{R}^2$. Then \wedge is an action of the group $\text{GL}(2)$ on the set \mathbb{R}^2 .

Proof We check the group action axioms.

GA1 Closure

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2)$ and let $(x, y) \in \mathbb{R}^2$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \wedge (x, y) = (ax + by, cx + dy) \in \mathbb{R}^2.$$

Thus axiom GA1 holds.

GA2 Identity

The identity element of the group $\text{GL}(2)$ is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $(x, y) \in \mathbb{R}^2$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (1x + 0y, 0x + 1y) = (x, y).$$

Thus axiom GA2 holds.

GA3 Composition

Let $\begin{pmatrix} p & q \\ r & s \end{pmatrix}, \begin{pmatrix} t & u \\ v & w \end{pmatrix} \in \text{GL}(2)$ and let $(x, y) \in \mathbb{R}^2$. We have to show that

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \wedge \left(\begin{pmatrix} t & u \\ v & w \end{pmatrix} \wedge (x, y) \right) = \left(\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} t & u \\ v & w \end{pmatrix} \right) \wedge (x, y).$$

Now

$$\begin{aligned} & \begin{pmatrix} p & q \\ r & s \end{pmatrix} \wedge \left(\begin{pmatrix} t & u \\ v & w \end{pmatrix} \wedge (x, y) \right) \\ &= \begin{pmatrix} p & q \\ r & s \end{pmatrix} \wedge (tx + uy, vx + wy) \quad (\text{by the definition of } \wedge) \\ &= (p(tx + uy) + q(vx + wy), r(tx + uy) + s(vx + wy)) \\ & \quad (\text{by the definition of } \wedge) \\ &= (ptx + puy + qvx + qwy, rtx + ruy + svx + swy) \end{aligned}$$

and

$$\begin{aligned} & \left(\begin{pmatrix} p & q \\ r & s \end{pmatrix} \times \begin{pmatrix} t & u \\ v & w \end{pmatrix} \right) \wedge (x, y) \\ &= \begin{pmatrix} pt + qv & pu + qw \\ rt + sv & ru + sw \end{pmatrix} \wedge (x, y) \\ &= ((pt + qv)x + (pu + qw)y, (rt + sv)x + (ru + sw)y) \\ & \quad (\text{by the definition of } \wedge) \\ &= (ptx + qvx + puy + qwy, rtx + svx + ruy + swy) \\ &= (ptx + puy + qvx + qwy, rtx + ruy + svx + swy) \\ & \quad (\text{by rearranging the terms}). \end{aligned}$$

The two expressions obtained are the same, so axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action. ■

Matrix multiplication is just one of many ways in which a group of 2×2 matrices with real entries can act on the plane \mathbb{R}^2 . We now look at some other examples.

Worked Exercise E60

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}$$

and consider the group (G, \times) and the plane \mathbb{R}^2 . Let \wedge be defined by

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge (x, y) = (ax, ay)$$

for all $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. Show that \wedge is a group action.

(You saw that G is a subgroup of $\text{GL}(2)$ in Exercise E21(a) in Unit E1, where it was denoted by M .)

Solution

We check the group action axioms.

GA1 Closure

The element (ax, ay) is an element of \mathbb{R}^2 for all real numbers a, x and y , so axiom GA1 holds.

GA2 Identity

The identity element of the group G is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $(x, y) \in \mathbb{R}^2$. Then $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (1x, 1y) = (x, y)$.

Thus axiom GA2 holds.

GA3 Composition

Let $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in G$ and let $(x, y) \in \mathbb{R}^2$.

We have to show that

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge \left(\begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \wedge (x, y) \right) = \left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \right) \wedge (x, y).$$

Now

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge \left(\begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \wedge (x, y) \right) &= \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge (cx, cy) \\ &= (acx, acy) \end{aligned}$$

and

$$\begin{aligned} \left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \right) \wedge (x, y) &= \begin{pmatrix} ac & ad + bc \\ 0 & ac \end{pmatrix} \wedge (x, y) \\ &= (acx, acy). \end{aligned}$$

The two expressions obtained are the same, so axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

Exercise E143

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

It is straightforward to show that G is a group under matrix multiplication, and you may assume this. (One of the additional exercises on Section 2 of Unit E1 asks you to show it.)

Determine which of the following, where $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ and $(x, y) \in \mathbb{R}^2$, define a group action of (G, \times) on \mathbb{R}^2 .

- (a) $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (ax, y)$
- (b) $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (ax, by)$
- (c) $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (ax, by + y)$

2 Orbits and stabilisers

In this section you will meet the ideas of *orbits* and *stabilisers* for a group action. These ideas will be used throughout the rest of the unit.

2.1 Orbits

To illustrate the idea of an *orbit*, consider the action of the group $S(\square)$ (see Figure 23) on the set $\{R, S, T, U\}$ of lines of symmetry of the square, shown in Figure 24. This is a group action by Theorem E59, as you saw in Exercise E137(f) in Subsection 1.2.



Figure 24 The lines of symmetry of the square

Let us choose a particular element of the set $\{R, S, T, U\}$, say R , and consider which elements of the set can be obtained from this element under the action of $S(\square)$.

- If we map R using e , b , r or t , then we obtain R .
- If we map R using a , c , s or u , then we obtain T .

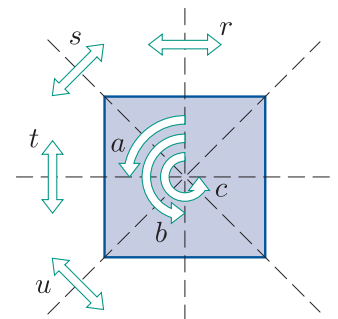


Figure 23 $S(\square)$

So under the action of $S(\square)$ the element R is mapped to R and T but to no other element. We say that the *orbit* of R under this group action is $\{R, T\}$, and we write $\text{Orb } R = \{R, T\}$.

Here is the general definition of an *orbit*.

Definition

Let \wedge be an action of a group G on a set X , and let x be an element of X . The **orbit** of x under \wedge , denoted by $\text{Orb } x$, is

$$\text{Orb } x = \{g \wedge x : g \in G\}.$$

That is, $\text{Orb } x$ is the set of elements of X that can be obtained from x under the action of G .

So, if a group G acts on a set X , then the orbit $\text{Orb } x$ of an element x of X is the subset of X that we obtain if we act on x using each element of G in turn. This is illustrated in Figure 25.

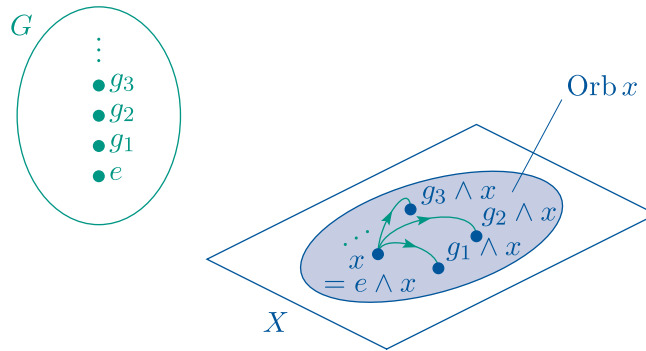


Figure 25 The orbit of an element x

Keep in mind that, as illustrated in Figure 25, $\text{Orb } x$ is a subset of the set X involved in the group action, not a subset of the group G .

As illustrated in Figure 25, the orbit $\text{Orb } x$ of a set element x under a group action always contains the element x itself. This is because $x = e \wedge x$ where e is the identity element of the group G that is acting, by axiom GA2.

In the worked exercise below we find the orbit of another set element under the action of $S(\square)$ on the lines of symmetry of the square.

Worked Exercise E61

Find $\text{Orb } S$ for the action of the group $S(\square)$ (see Figure 26) on the set $\{R, S, T, U\}$ of lines of symmetry of the square (shown on a single diagram in Figure 27).

Solution

We have

$$\begin{aligned}\text{Orb } S &= \{g \wedge S : g \in S(\square)\} \\ &= \{e \wedge S, a \wedge S, b \wedge S, c \wedge S, r \wedge S, s \wedge S, t \wedge S, u \wedge S\} \\ &= \{S, U, S, U, U, S, U, S\} \\ &= \{S, U\}.\end{aligned}$$

If we are dealing with an action of a *group of symmetries*, then we can usually quickly write down the orbit of a set element just by considering the effects of the symmetries, as demonstrated below.

Worked Exercise E62

Consider again the action of the group $S(\square)$ (see Figure 26) on the set $\{R, S, T, U\}$ of lines of symmetry of the square (see Figure 27). Write down the orbit of each of R , S , T and U .

Solution

There are symmetries of the square that map R to R and to T , but none that map R to S or U . Thus $\text{Orb } R = \{R, T\}$. We can find the orbits of the other lines of symmetry in a similar way.

The orbits are

$$\begin{aligned}\text{Orb } R &= \{R, T\}, \\ \text{Orb } S &= \{S, U\}, \\ \text{Orb } T &= \{R, T\}, \\ \text{Orb } U &= \{S, U\}.\end{aligned}$$

Exercise E144

Consider the action of the group $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 28). Write down the orbit of each vertex label.

(This mapping effect was shown to be a group action immediately following Exercise E137 in Subsection 1.2.)

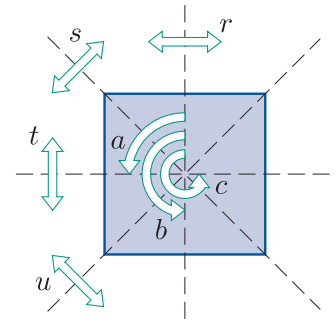


Figure 26 $S(\square)$

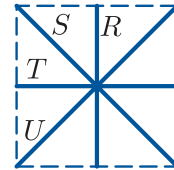


Figure 27 The lines of symmetry of the square

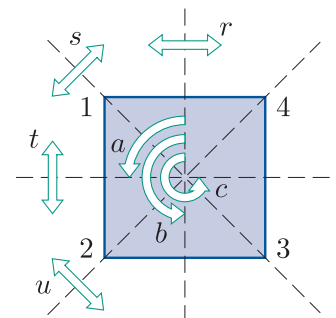


Figure 28 $S(\square)$

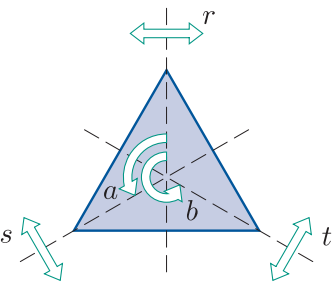


Figure 29 $S(\triangle)$

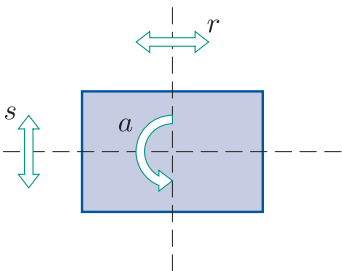
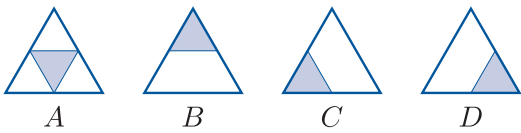


Figure 30 $S(\square)$

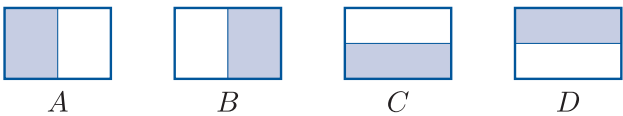
Exercise E145

Consider the action of the group $S(\triangle)$ (see Figure 29) on the set $\{A, B, C, D\}$ of modified triangles shown below. Write down the orbit of each of A , B , C and D .



Exercise E146

Consider the action of the group $S(\square)$ (see Figure 30) on the set $\{A, B, C, D\}$ of modified rectangles shown below. Write down the orbit of each of A , B , C and D .



In the next worked exercise we find the orbits of set elements under the action of an infinite group.

Worked Exercise E63

Consider the action of the group $S^+(\circ)$ of direct symmetries of the disc on the plane \mathbb{R}^2 , assuming that the disc is placed with its centre at the origin O . Describe geometrically the orbit of each point in \mathbb{R}^2 .

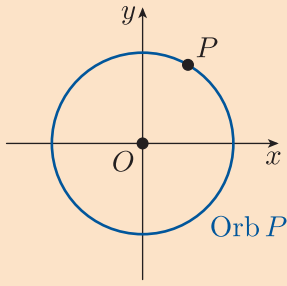
Solution

☁ The group $S^+(\circ)$ is the group of rotations about the origin O . ☁

Any rotation about O maps O to itself, so

$$\text{Orb } O = \{O\}.$$

Now let P be any other point in \mathbb{R}^2 . The elements of $S^+(\circ)$ rotate P about O , through all possible angles. So $\text{Orb } P$ is the circle with centre O whose radius is the distance between O and P , as shown below.



Exercise E147

Consider the action of the group $S(\bigcirc)$ of *all* symmetries of the disc on the plane \mathbb{R}^2 , assuming that the disc is placed with its centre at the origin O . Describe geometrically the orbit of each point in \mathbb{R}^2 .

(Remember that the elements of $S(\bigcirc)$ are the rotations about O and the reflections in the lines through O .)

You may have noticed that in all the examples of orbits that you have met so far, the orbits of any two different elements of the set involved are always either *identical sets* or *disjoint sets*: they never partially overlap. For example, consider the orbits of the lines of symmetry R, S, T and U of the square under the action of the group $S(\square)$, which were found in Worked Exercise E62:

$$\text{Orb } R = \{R, T\},$$

$$\text{Orb } S = \{S, U\},$$

$$\text{Orb } T = \{R, T\},$$

$$\text{Orb } U = \{S, U\}.$$

Here, for instance, $\text{Orb } R$ and $\text{Orb } T$ are the same set, while $\text{Orb } R$ and $\text{Orb } S$ are disjoint sets.

Also, under any group action, every element of the set involved lies in some orbit. This is because every element of the set lies in its own orbit, at least.

So, in all the examples that you have met, the distinct orbits form a *partition* of the set on which the group acts. For example, the distinct orbits under the action of the group $S(\square)$ on the set $\{R, S, T, U\}$ of lines of symmetry of the square form the following partition of the set $\{R, S, T, U\}$:

$$\{R, T\}, \quad \{S, U\}.$$

The distinct orbits under a group action always form a partition of the set on which the group acts, as proved below.

Theorem E62

Let \wedge be an action of a group (G, \circ) on a set X . Then the distinct orbits of the elements of X under \wedge form a partition of X .

Proof To prove the theorem, we define a relation \sim on X , prove that \sim is an equivalence relation, and show that its equivalence classes are the distinct orbits under \wedge of the elements of X . (There is a reminder of the definition of an equivalence relation in Subsection 4.1 of Unit E1.)

Let the relation \sim be defined on X by

$$x \sim y \quad \text{if } y \in \text{Orb } x.$$

To prove that \sim is an equivalence relation, we show that \sim has the reflexive, symmetric and transitive properties. Let the identity element of (G, \circ) be e .

E1 Reflexivity

Let $x \in X$. We have to show that $x \sim x$. That is, we have to show that

$$x \in \text{Orb } x.$$

This is true (as mentioned earlier), because $x = e \wedge x$. So $x \sim x$. Thus \sim is reflexive.

E2 Symmetry

Let $x, y \in X$, and suppose that $x \sim y$. Then

$$y \in \text{Orb } x.$$

We have to show that $y \sim x$, that is, $x \in \text{Orb } y$.

Since $y \in \text{Orb } x$, there is an element g in G such that

$$y = g \wedge x.$$

Hence

$$\begin{aligned} g^{-1} \wedge y &= g^{-1} \wedge (g \wedge x) \\ &= (g^{-1} \circ g) \wedge x \quad (\text{by axiom GA3}) \\ &= e \wedge x \\ &= x \quad (\text{by axiom GA2}). \end{aligned}$$

Since $x = g^{-1} \wedge y$ and $g^{-1} \in G$, we have $x \in \text{Orb } y$, and hence $y \sim x$. Thus \sim is symmetric.

GA3 Transitivity

Let $x, y, z \in X$, and suppose that $x \sim y$ and $y \sim z$; that is,

$$y \in \text{Orb } x \quad \text{and} \quad z \in \text{Orb } y.$$

We have to show that $x \sim z$, that is, $z \in \text{Orb } x$.

Since $y \in \text{Orb } x$ and $z \in \text{Orb } y$, there are elements g and h in G such that

$$y = g \wedge x \quad \text{and} \quad z = h \wedge y.$$

Hence

$$\begin{aligned} z &= h \wedge y \\ &= h \wedge (g \wedge x) \quad (\text{since } y = g \wedge x) \\ &= (h \circ g) \wedge x \quad (\text{by axiom GA3}). \end{aligned}$$

Since $z = (h \circ g) \wedge x$ and $h \circ g \in G$, we have $z \in \text{Orb } x$, that is, $x \sim z$. Thus \sim is transitive.

Hence \sim has the reflexive, symmetric and transitive properties, so it is an equivalence relation on X .

The equivalence classes of any equivalence relation form a partition of the set on which the relation is defined (by Theorem A16, restated in Subsection 4.1 of Unit E1). Hence the equivalence classes of \sim form a partition of X . But the equivalence class of any element x of X is

$$\{y \in X : x \sim y\} = \{y \in X : y \in \text{Orb } x\} = \text{Orb } x.$$

Thus the equivalence classes are precisely the distinct orbits under \wedge , so the orbits form a partition of X . ■

The part of the proof of Theorem E62 that deals with the symmetric property shows that for any group action \wedge ,

$$\text{if } y = g \wedge x, \text{ then } x = g^{-1} \wedge y.$$

This is a useful result that is worth remembering.

We refer to the distinct orbits of elements under a group action as the *orbits of the group action*. Theorem E62 gives us the following strategy for finding the orbits of a group action on a finite set.

Strategy E7

To find the orbits of an action of a group G on a finite set X , do the following.

1. Choose any element x of X , and find its orbit.
2. Choose any element of X not yet assigned to an orbit, and find its orbit.
3. Repeat step 2 until X is partitioned.

We can also use Strategy E7 to find the orbits of an action of a group G on an *infinite* set X when there are only finitely many orbits.

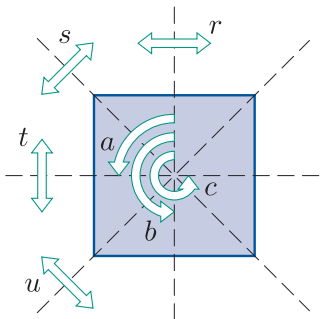
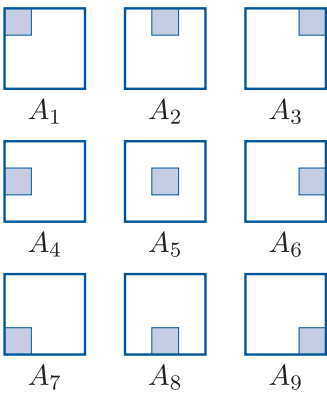


Figure 31 $S(\square)$

Exercise E148

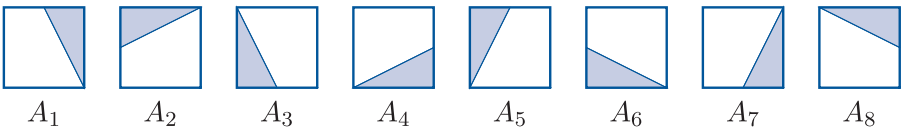
Consider the action of the group $S(\square)$ (see Figure 31) on the set $\{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9\}$ of modified squares shown below. Write down the orbits of this group action.



(This is a group action by Theorem E59.)

Exercise E149

(a) Consider the action of the group $S^+(\square)$ of direct symmetries of the square on the set $X = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8\}$ of modified squares shown below. Write down the orbits of this group action.



(b) Now consider the action of the group $S(\square)$ of *all* symmetries of the square on the same set X as in part (a). Write down the orbits of this group action.

(These are group actions by Theorem E59.)

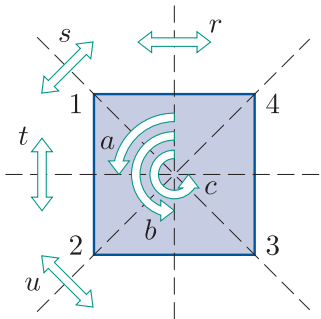


Figure 32 $S(\square)$

Exercise E150

Consider the action of each of the following subgroups of $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 32). For the action of each subgroup, write down the orbits.

(Each subgroup gives a group action by Theorem E59.)

- (a) $S^+(\square)$ (b) $\{e, b, s, u\}$ (c) $\{e, r\}$ (d) $\{e\}$

2.2 Orbits of group actions on \mathbb{R}^2

Worked Exercise E63 in the previous subsection involved the action of a group on the plane \mathbb{R}^2 . Because the set involved was the plane \mathbb{R}^2 , we were able to give a geometric description of the orbits of the action: they were the origin and the circles whose centre is the origin. These orbits partition the plane \mathbb{R}^2 , as we know they must by Theorem E62: some of them are shown in Figure 33.

In this subsection we will find the orbits of some more actions of groups on the plane \mathbb{R}^2 . Many of the groups involved are matrix groups.

In the first worked exercise we find the orbits of some individual points in \mathbb{R}^2 under a group action.

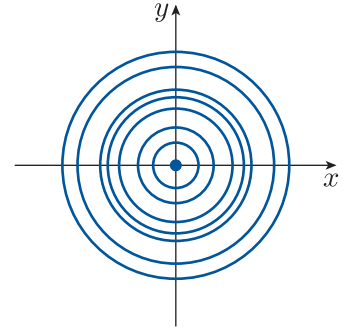


Figure 33 Some of the orbits of the group action in Worked Exercise E63

Worked Exercise E64

Let

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R}^+ \right\}.$$

Consider the action \wedge of the group (G, \times) on the set \mathbb{R}^2 defined by


$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \wedge (x, y) = (ax, by)$$

for all $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. (You may assume that (G, \times) is a group and that \wedge is a group action; both of these are straightforward to show.)

Find the orbit of each of the following points in \mathbb{R}^2 . Describe each of these orbits geometrically.

- (a) $(0, 0)$ (b) $(-1, 0)$ (c) $(1, -1)$


Solution

 First we find an expression for the orbit of a general point (x, y) in \mathbb{R}^2 under this group action.

We have to apply the general definition of an orbit,

$$\text{Orb } x = \{g \wedge x : g \in G\},$$

to the situation here. We

- replace x by a general element of the set \mathbb{R}^2 , say (x, y)
- replace g by a general element of the group G , say $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. 

For any point $(x, y) \in \mathbb{R}^2$,

$$\text{Orb}(x, y) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \wedge (x, y) : \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G \right\}$$

Now we use the definition of \wedge to simplify the expression in front of the colon. We also simplify the condition after the colon: what it tells us about the values taken by a and b is simply that $a, b \in \mathbb{R}^+$.

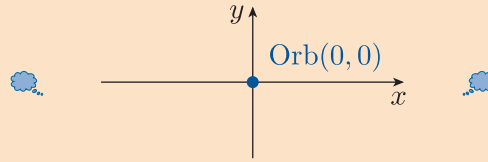
$$= \{(ax, by) : a, b \in \mathbb{R}^+\}.$$

We now have an expression for the orbit of a general point (x, y) . We use it to find the orbits of the given points.

(a) Putting $(x, y) = (0, 0)$ gives

$$\begin{aligned} \text{Orb}(0, 0) &= \{(a \times 0, b \times 0) : a, b \in \mathbb{R}^+\} \\ &= \{(0, 0) : a, b \in \mathbb{R}^+\} \\ &= \{(0, 0)\}. \end{aligned}$$

So $\text{Orb}(0, 0)$ consists of the origin alone.

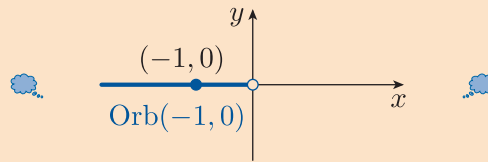


(b) Putting $(x, y) = (-1, 0)$ gives

$$\begin{aligned} \text{Orb}(-1, 0) &= \{(a \times (-1), b \times 0) : a, b \in \mathbb{R}^+\} \\ &= \{(-a, 0) : a \in \mathbb{R}^+\}. \end{aligned}$$

As a runs through all the values in \mathbb{R}^+ , the point $(-a, 0)$ moves through all the points on the negative part of the x -axis.

So $\text{Orb}(-1, 0)$ is the negative part of the x -axis.

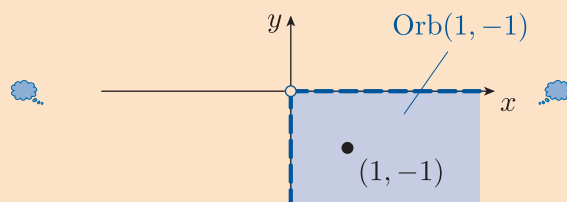


(c) Putting $(x, y) = (1, -1)$ gives

$$\begin{aligned} \text{Orb}(1, -1) &= \{(a \times 1, b \times (-1)) : a, b \in \mathbb{R}^+\} \\ &= \{(a, -b) : a, b \in \mathbb{R}^+\}. \end{aligned}$$

As a and b run through all the values in \mathbb{R}^+ , the point $(a, -b)$ moves through all the points in the fourth quadrant of the plane.

So $\text{Orb}(1, -1)$ is the fourth quadrant of the plane. (It does not include any points on the x -axis or y -axis.)



Exercise E151

For the group action in Worked Exercise E64, find the orbit of each of the following points. Describe each of these orbits geometrically.

- (a) $(1, 0)$ (b) $(0, -1)$ (c) $(1, 1)$

We have now found six of the orbits of the group action in Worked Exercise E64 and Exercise E151. These orbits are illustrated in Figure 34.

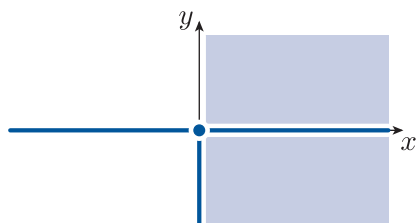


Figure 34 Six of the orbits of the group action in Worked Exercise E64 and Exercise E151

Exercise E152

Find the remaining orbits of the group action in Worked Exercise E64 and Exercise E151, remembering that the orbits partition the plane. Sketch a diagram to show how the orbits partition the plane.

The group action considered in Worked Exercise E64 and the two subsequent exercises has only finitely many orbits (nine altogether). In contrast, the group action in the next worked exercise has infinitely many.

Finding all the orbits of a group action can be quite complicated. Usually it is best to start by finding an expression for the orbit of a general element of the set on which the group acts, as was done in Worked Exercise E64. Next, it is often helpful to use this expression to find the

orbits of a few particular elements of the set, to try to get an idea of how the set might split up into orbits. Finally, you can attempt to confirm what you think happens by using algebraic or geometric arguments. Keep in mind that the orbits partition the set on which the group acts, so to find more orbits you need to consider elements that do not lie in the orbits that you have already found.

Worked Exercise E65

Consider the action \wedge of the group $(\mathbb{R}, +)$ on the set \mathbb{R}^2 defined by

$$g \wedge (x, y) = (x + yg, y)$$

for all $g \in \mathbb{R}$ and all $(x, y) \in \mathbb{R}^2$.

(You saw that this is a group action in Worked Exercise E59 in Subsection 1.3.)


Find all the orbits of this group action. Describe them geometrically, and sketch a diagram to show how they partition the plane.

Solution


 We start by finding an expression for the orbit of a general point (x, y) under this group action. 

For any point $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned}\text{Orb}(x, y) &= \{g \wedge (x, y) : g \in \mathbb{R}\} \\ &= \{(x + yg, y) : g \in \mathbb{R}\}.\end{aligned}$$

 Let us use this equation to find the orbits of some points, to try to get an idea of what might happen in general. We choose ‘simple’ points to start with. We have, for example,

$$\begin{aligned}\text{Orb}(0, 0) &= \{(0 + 0g, 0) : g \in \mathbb{R}\} = \{(0, 0) : g \in \mathbb{R}\} = \{(0, 0)\}, \\ \text{Orb}(1, 0) &= \{(1 + 0g, 0) : g \in \mathbb{R}\} = \{(1, 0) : g \in \mathbb{R}\} = \{(1, 0)\}.\end{aligned}$$

The working here leads us to realise that any point of the form $(x, 0)$ has an orbit that contains only the point itself. We confirm this formally. 

For any point $(x, 0)$, that is, any point on the x -axis, we have

$$\text{Orb}(x, 0) = \{(x + 0g, 0) : g \in \mathbb{R}\} = \{(x, 0) : g \in \mathbb{R}\} = \{(x, 0)\}.$$

 Now let us try some other points. We have, for example,

$$\begin{aligned}\text{Orb}(0, 1) &= \{(0 + 1g, 1) : g \in \mathbb{R}\} = \{(g, 1) : g \in \mathbb{R}\}, \\ \text{Orb}(0, 2) &= \{(0 + 2g, 2) : g \in \mathbb{R}\} = \{(2g, 2) : g \in \mathbb{R}\}.\end{aligned}$$

As g runs through all values in \mathbb{R} , the point $(g, 1)$ moves through all the points on the horizontal line with y -intercept 1. So $\text{Orb}(0, 1)$ is the horizontal line through $(0, 1)$. Similarly, as g runs through all

values in \mathbb{R} , the point $(2g, 2)$ moves through all the points on the horizontal line with y -intercept 2. So $\text{Orb}(0, 2)$ is the horizontal line through $(0, 2)$. It looks as if the orbit of any point of the form $(0, y)$, where $y \neq 0$, is the horizontal line through that point. We now check this formally. 🧠

For any point $(0, y)$ with $y \neq 0$, that is, any point on the y -axis except the origin, we have

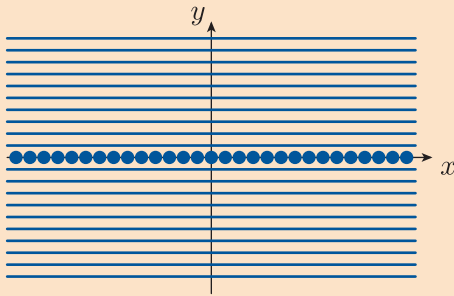
$$\text{Orb}(0, y) = \{(0 + yg, y) : g \in \mathbb{R}\} = \{(yg, y) : g \in \mathbb{R}\}.$$

This is the set of points that lie on the horizontal line through $(0, y)$. So $\text{Orb}(0, y)$, where $y \neq 0$, is the horizontal line through $(0, y)$.

🧠 We have now found all the orbits. 🧠

Every point in \mathbb{R}^2 is either a point on the x -axis or a point on a horizontal line through some point of the form $(0, y)$, where $y \neq 0$. So we have now partitioned the plane \mathbb{R}^2 into orbits.

The orbits are the individual points on the x -axis, together with all the horizontal lines other than the x -axis, as sketched below.



Exercise E153

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Consider the action \wedge of the group (G, \times) on the set \mathbb{R}^2 defined by

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (ax, y)$$

for all $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. (You saw that this is a group action in Exercise E143(a) in Subsection 1.4.)

Find all the orbits of this group action. Describe them geometrically, and sketch a diagram to show how they partition the plane.

Exercise E154

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Consider the action \wedge of the group (G, \times) on the set \mathbb{R}^2 defined by

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge (x, y) = (ax, ay)$$

for all $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. (You saw that this is a group action in Worked Exercise E60 in Subsection 1.4.)

Find all the orbits of this group action. Describe them geometrically, and sketch a diagram to show how they partition the plane.

2.3 Stabilisers

This subsection introduces the idea of a *stabiliser*.

Definition

Let \wedge be an action of a group G on a set X , and let x be an element of X . The **stabiliser** of x under \wedge , denoted by $\text{Stab } x$, is given by

$$\text{Stab } x = \{g \in G : g \wedge x = x\}.$$

That is, $\text{Stab } x$ is the set of elements of G that fix x .

In other words, if a group G acts on a set X and x is an element of X , then the stabiliser $\text{Stab } x$ of x is the set of elements of G that map x to itself. This is illustrated in Figure 35.

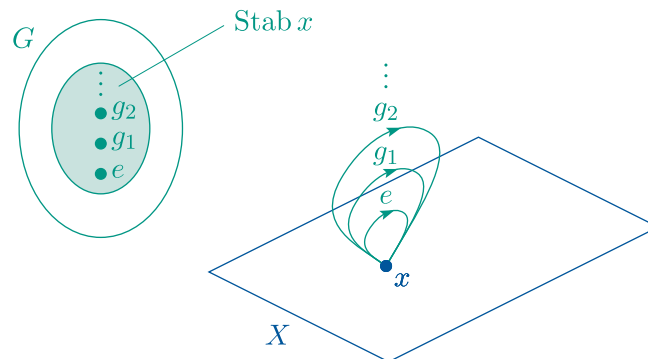


Figure 35 The stabiliser of an element x

Notice that, whereas the orbit of an element x is a subset of the set X , the stabiliser of x is a subset of the group G .

As illustrated in Figure 35, the stabiliser $\text{Stab } x$ of a set element x under the action of a group always contains the identity element e of the group. This is because $e \wedge x = x$, by axiom GA2.

Worked Exercise E66

Find $\text{Stab } R$ for the action of the group $S(\square)$ (see Figure 36) on the set $\{R, S, T, U\}$ of lines of symmetry of the square (see Figure 37).

Solution

We have

$$e \wedge R = R,$$

$$a \wedge R = T,$$

$$b \wedge R = R,$$

$$c \wedge R = T,$$

$$r \wedge R = R,$$

$$s \wedge R = T,$$

$$t \wedge R = R,$$

$$u \wedge R = T.$$

☁ The elements of $S(\square)$ that fix R are e, b, r and t . ☁

Hence

$$\text{Stab } R = \{e, b, r, t\}.$$

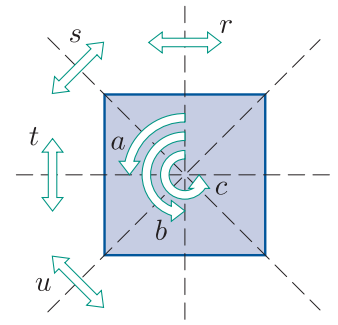


Figure 36 $S(\square)$

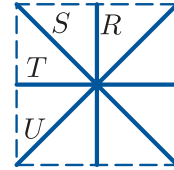


Figure 37 The lines of symmetry of the square

As with orbits, if we are dealing with the action of a group of symmetries, then we can usually quickly write down the stabilisers of set elements just by considering the effects of the symmetries.

Worked Exercise E67

Consider the action of the group $S(\square)$ (see Figure 36) on the set $\{R, S, T, U\}$ of lines of symmetry of the square (see Figure 37). Write down the stabiliser of each of R, S, T and U .

Solution

☁ The symmetries e, b, r and t all map R to itself, but none of the other symmetries do. Hence $\text{Stab } R = \{e, b, r, t\}$. The stabilisers of the other lines of symmetry can be found in a similar way. ☁

The stabilisers are

$$\text{Stab } R = \{e, b, r, t\},$$

$$\text{Stab } S = \{e, b, s, u\},$$

$$\text{Stab } T = \{e, b, r, t\},$$

$$\text{Stab } U = \{e, b, s, u\}.$$

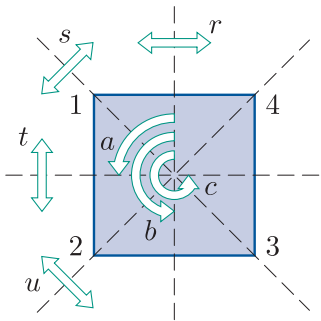


Figure 38 $S(\square)$

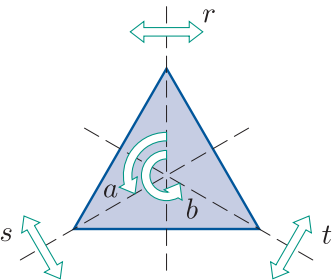


Figure 39 $S(\triangle)$

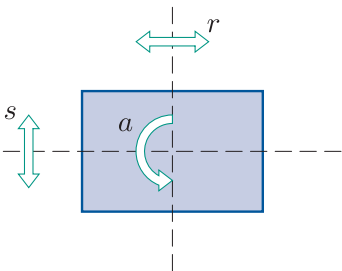


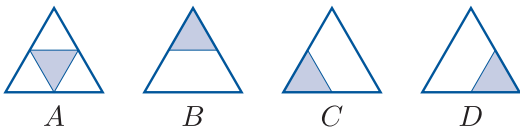
Figure 40 $S(\square)$

Exercise E155

Consider the action of the group $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 38). Write down the stabiliser of each vertex label.

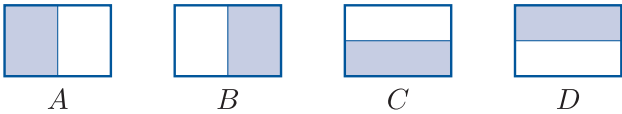
Exercise E156

Consider the action of the group $S(\triangle)$ (see Figure 39) on the set $\{A, B, C, D\}$ of modified triangles shown below. Write down the stabiliser of each of A , B , C and D .



Exercise E157

Consider the action of the group $S(\square)$ (see Figure 40) on the set $\{A, B, C, D\}$ of modified rectangles shown below. Write down the stabiliser of each of A , B , C and D .



The next worked exercise involves an action of an infinite group.

Worked Exercise E68

Consider the action of the group $S^+(\circ)$ of direct symmetries of the disc on the plane \mathbb{R}^2 , assuming that the disc is placed with its centre at the origin O . Find the stabiliser of each point in \mathbb{R}^2 .

Solution

The group $S^+(\circ)$ is the group of rotations about the origin O . Any rotation about O fixes O , so $\text{Stab } O$ is the whole of $S^+(\circ)$. Now let P be any other point in \mathbb{R}^2 . The only rotation in $S^+(\circ)$ that fixes P is the identity symmetry e (also denoted by r_0). So $\text{Stab } P = \{e\}$.

Exercise E158

Consider the action of the group $S(\bigcirc)$ of *all* symmetries of the disc on the plane \mathbb{R}^2 , assuming that the disc is placed with its centre at the origin O . Find the stabiliser of each point in \mathbb{R}^2 .

You might have noticed that every example of a stabiliser that you have met so far has turned out to be a *subgroup* of the group that is acting, rather than just a subset of the group. For example, consider the stabilisers of the lines of symmetry R , S , T and U of the square (see Figure 41) under the action of the group $S(\square)$ (see Figure 42), which were found in Worked Exercise E67:

$$\text{Stab } R = \{e, b, r, t\},$$

$$\text{Stab } S = \{e, b, s, u\},$$

$$\text{Stab } T = \{e, b, r, t\},$$

$$\text{Stab } U = \{e, b, s, u\}.$$

Both $\{e, b, r, t\}$ and $\{e, b, s, u\}$ are subgroups of $S(\square)$, as you saw in Exercise E15 in Subsection 1.4 of Unit E1.

The stabiliser of a set element under the action of a group is always a subgroup of the group that is acting, as proved below.

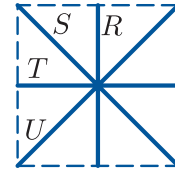


Figure 41 The lines of symmetry of the square

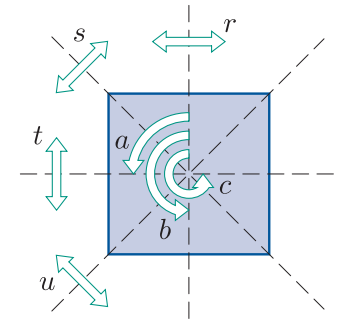


Figure 42 $S(\square)$

Theorem E63

Let \wedge be an action of a group (G, \circ) on a set X . Then, for each element x of X , the set $\text{Stab } x$ is a subgroup of (G, \circ) .

Proof Let x be an element of X . We show that the three subgroup properties hold for $\text{Stab } x$.

SG1 Closure

Let $g, h \in \text{Stab } x$. Then

$$g \wedge x = x \quad \text{and} \quad h \wedge x = x.$$

We have

$$\begin{aligned} (g \circ h) \wedge x &= g \wedge (h \wedge x) \quad (\text{by axiom GA3}) \\ &= g \wedge x \\ &= x. \end{aligned}$$

Hence $g \circ h \in \text{Stab } x$. Thus property SG1 holds.

SG2 Identity

Let e be the identity element of (G, \circ) . Since $e \wedge x = x$, by axiom GA2, it follows that $e \in \text{Stab } x$. Thus property SG2 holds.

SG3 Inverses

Let $g \in \text{Stab } x$. Then

$$g \wedge x = x.$$

It follows that

$$\begin{aligned} g^{-1} \wedge x &= g^{-1} \wedge (g \wedge x) \\ &= (g^{-1} \circ g) \wedge x \quad (\text{by axiom GA3}) \\ &= e \wedge x \\ &= x \quad (\text{by axiom GA2}). \end{aligned}$$

Hence $g^{-1} \in \text{Stab } x$. Thus property SG3 holds.

Since the three subgroup properties hold, $\text{Stab } x$ is a subgroup of G .

Exercise E159

Consider again the action of the group $S(\square)$ (see Figure 43) on the set $\{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9\}$ of modified squares shown below. Write down the stabiliser of each of the modified squares, and check that each of these stabilisers is a subgroup of $S(\square)$.

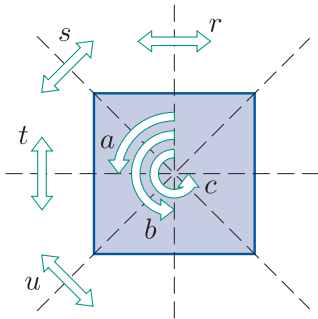
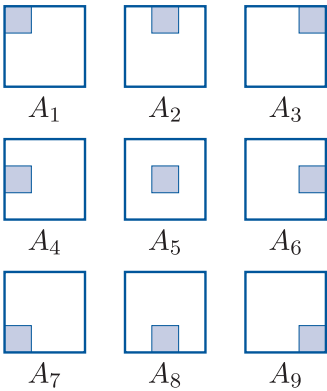
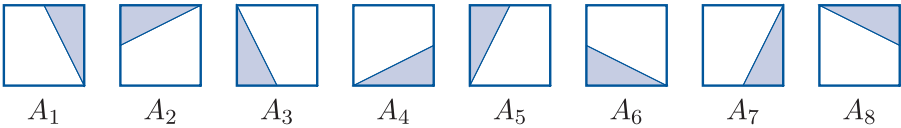


Figure 43 $S(\square)$



Exercise E160

- (a) Consider the action of the group $S^+(\square)$ of direct symmetries of the square on the set $X = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8\}$ of modified squares shown below. Write down the stabiliser of each of the modified squares under this group action, and check that each of these stabilisers is a subgroup of $S(\square)$.



- (b) Now consider the group action of the group $S(\square)$ of all symmetries of the square on the same set X as in part (a). Write down the stabiliser of each of the modified squares under this group action, and check that each of these stabilisers is a subgroup of $S(\square)$.

2.4 Stabilisers of group actions on \mathbb{R}^2

In this subsection we will find stabilisers under the group actions on the plane \mathbb{R}^2 that we considered in Subsection 2.2.

Worked Exercise E69

Let

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R}^+ \right\}.$$

Consider the action \wedge of the group (G, \times) on the set \mathbb{R}^2 defined by


$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \wedge (x, y) = (ax, by)$$

for all $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. (As in Worked Exercise E64 in Subsection 2.2, you may assume that (G, \times) is a group and that \wedge is a group action.)

Find the stabiliser of each of the following points in \mathbb{R}^2 .

- (a) $(0, 0)$ (b) $(-1, 0)$ (c) $(1, -1)$


Solution

 First we find an expression for the stabiliser of a general point (x, y) in \mathbb{R}^2 under this group action.

We have to apply the general definition of a stabiliser,



$$\text{Stab } x = \{g \in G : g \wedge x = x\},$$

to the situation here. We

- replace x by a general element of the set \mathbb{R}^2 , say (x, y)
- replace g by a general element of the group G , say $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. 

For any point $(x, y) \in \mathbb{R}^2$,



$$\text{Stab}(x, y) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \wedge (x, y) = (x, y) \right\}$$

 We use the definition of \wedge to simplify the condition after the colon. 

$$= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : (ax, by) = (x, y) \right\}$$

 We can rewrite the condition slightly. 

$$= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : ax = x \text{ and } by = y \right\}.$$

 We now have an expression for the stabiliser of a general point (x, y) . We use it to find the stabilisers of the given points. 

(a) Putting $(x, y) = (0, 0)$ gives

$$\begin{aligned} \text{Stab}(0, 0) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a \times 0 = 0 \text{ and } b \times 0 = 0 \right\} \\ &= G. \end{aligned}$$

(b) Putting $(x, y) = (-1, 0)$ gives

$$\begin{aligned} \text{Stab}(-1, 0) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a \times (-1) = -1 \text{ and } b \times 0 = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : -a = -1 \text{ and } 0 = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a = 1 \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} : b \in \mathbb{R}^+ \right\}. \end{aligned}$$

(c) Putting $(x, y) = (1, -1)$ gives

$$\begin{aligned} \text{Stab}(1, -1) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a \times 1 = 1 \text{ and } b \times (-1) = -1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a = 1 \text{ and } b = 1 \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}. \end{aligned}$$

Notice that the answers to parts (a) and (c) of Worked Exercise E69 are groups under matrix multiplication, as expected in view of Theorem E63. The answer to part (b) is also guaranteed to be a group under matrix multiplication, by the same theorem.

Exercise E161

For the group action in Worked Exercise E69, find the stabiliser of each of the following points.

- (a) $(2, 0)$ (b) $(0, 5)$

For a group action on the plane \mathbb{R}^2 , such as the group action in Worked Exercise E69 and Exercise E161, we cannot of course list the stabiliser of every point in \mathbb{R}^2 individually, since there are infinitely many points. However, we can often determine that the stabiliser of each point of a particular form is a certain subgroup of the group that is acting, and the stabiliser of each point of another form is another subgroup of the group, and so on. In this way we may be able to describe the stabiliser of every point in \mathbb{R}^2 .

In the next exercise you are asked to do this for the group action in Worked Exercise E69 and Exercise E161.

Exercise E162

Consider the group action in Worked Exercise E69 and Exercise E161.

It was found in Worked Exercise E69 that the stabiliser of the origin is the whole group (G, \times) .

- Show that the stabiliser of every point of the form $(x, 0)$ where $x \in \mathbb{R}^*$ (that is, every point on the x -axis except the origin) is the same subgroup of (G, \times) as found in Exercise E161(a).
- Show that the stabiliser of every point of the form $(0, y)$ where $y \in \mathbb{R}^*$ (that is, every point on the y -axis except the origin) is the same subgroup of (G, \times) as found in Exercise E161(b).
- Show that the stabiliser of every point of the form (x, y) where $x, y \in \mathbb{R}^*$ (that is, every point that lies neither on the x -axis nor on the y -axis) is the trivial subgroup of (G, \times) .

In the next worked exercise we find the stabiliser of every point in \mathbb{R}^2 under the group action whose orbits we found in Worked Exercise E65 in Subsection 2.2.

Worked Exercise E70



Consider the action of the group $(\mathbb{R}, +)$ on the set \mathbb{R}^2 defined by

$$g \wedge (x, y) = (x + yg, y)$$

for all $g \in \mathbb{R}$ and all $(x, y) \in \mathbb{R}^2$. (You saw that this is a group action in Worked Exercise E59 in Subsection 1.3.)



Find the stabiliser of each point in \mathbb{R}^2 .

Solution

 As in the previous worked exercise, we start by finding an expression for the stabiliser of a general point (x, y) under this group action. 

For any point $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned} \text{Stab}(x, y) &= \{g \in \mathbb{R} : g \wedge (x, y) = (x, y)\} \\ &= \{g \in \mathbb{R} : (x + yg, y) = (x, y)\} \\ &= \{g \in \mathbb{R} : x + yg = x \text{ and } y = y\} \\ &= \{g \in \mathbb{R} : x + yg = x\} \\ &= \{g \in \mathbb{R} : yg = 0\}. \end{aligned}$$

 We cannot simplify this specification of $\text{Stab}(x, y)$ any further for a general point (x, y) . However, for a point (x, y) in which y is non-zero, the condition $yg = 0$ simplifies to $g = 0$, which tells us that the only element of $\text{Stab}(x, y)$ is 0. So we now split into two cases: $y \neq 0$ and $y = 0$. 

Hence for any point $(x, y) \in \mathbb{R}^2$ with $y \neq 0$ (that is, any point not on the x -axis),

$$\begin{aligned} \text{Stab}(x, y) &= \{g \in \mathbb{R} : yg = 0\} \\ &= \{g \in \mathbb{R} : g = 0\} \quad (\text{since } y \neq 0) \\ &= \{0\}. \end{aligned}$$

Also, for any point $(x, 0) \in \mathbb{R}^2$ (that is, any point on the x -axis),

$$\begin{aligned} \text{Stab}(x, 0) &= \{g \in \mathbb{R} : 0g = 0\} \\ &= \{g \in \mathbb{R} : 0 = 0\} \\ &= \mathbb{R}. \end{aligned}$$

 We have now found the stabiliser of every point in \mathbb{R}^2 . 

In summary, the stabiliser of any point on the x -axis is the whole group \mathbb{R} , and the stabiliser of any other point is the trivial subgroup $\{0\}$.

If you are trying to find the stabiliser of each point in the plane \mathbb{R}^2 under a particular group action, and you have found an expression for the stabiliser of a general point (x, y) but are not sure how to proceed from there, then it can be helpful to use your expression to find the stabilisers of a few particular points, just as for orbits. This should help you develop ideas about what happens in general, and you can then try to confirm your ideas algebraically.

Exercise E163

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Consider the action of the group (G, \times) on the set \mathbb{R}^2 defined by

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (ax, y)$$

for all $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. (You saw that this is a group action in Exercise E143(a) in Subsection 1.4.)

Find the stabiliser of each point in \mathbb{R}^2 .

Exercise E164

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Consider the action of the group (G, \times) on the set \mathbb{R}^2 defined by

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge (x, y) = (ax, ay)$$

for all $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. (You saw that this is a group action in Worked Exercise E60 in Subsection 1.4.)

Find the stabiliser of each point in \mathbb{R}^2 .

3 The Orbit–Stabiliser Theorem

In this section you will meet the *Orbit–Stabiliser Theorem*, an important result that applies to actions of *finite* groups.

3.1 What is the Orbit–Stabiliser Theorem?

We begin with an exercise.

Exercise E165

Consider the action of the group $S(\square)$ (see Figure 44) on the set of all figures in \mathbb{R}^2 . Complete the following table, in which each row corresponds to the modified square A in \mathbb{R}^2 shown at the left of the row. Notice the apparent general relationship between $|\text{Orb } A|$ and $|\text{Stab } A|$, the numbers of elements in $\text{Orb } A$ and $\text{Stab } A$, respectively.

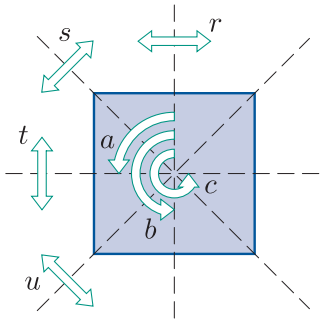


Figure 44 $S(\square)$

| A | $\text{Orb } A$ | $\text{Stab } A$ | $ \text{Orb } A $ | $ \text{Stab } A $ |
|-----|--|------------------|-------------------|--------------------|
| | $\{\text{square with diagonal from bottom-left to top-right}, \text{square with diagonal from top-left to bottom-right}\}$ | $\{e, b\}$ | 4 | 2 |
| | | | | |
| | | | | |
| | | | | |

In Exercise E165 you should have found that, for each modified square A in the table,

$$|\text{Orb } A| \times |\text{Stab } A| = 8.$$

That is, for each of these modified squares, multiplying the number of elements in its orbit by the number of elements in its stabiliser gives the order of the group $S(\square)$. These findings are instances of the following general theorem. It is proved in the next subsection.

Theorem E64 Orbit–Stabiliser Theorem

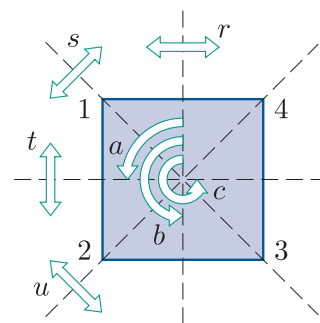
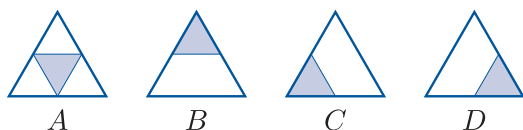
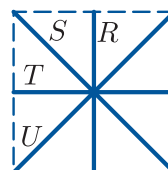
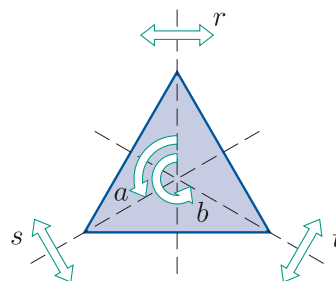
Suppose that the finite group G acts on the set X . Then, for each element x in X ,

$$|\text{Orb } x| \times |\text{Stab } x| = |G|.$$

Exercise E166

In each of parts (a), (b) and (c), verify the Orbit–Stabiliser Theorem for each element x of the set on which the group acts.

- (a) The action of $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 45).
- (b) The action of $S(\square)$ on the set $\{R, S, T, U\}$ of lines of symmetry of the square (see Figure 46).
- (c) The action of $S(\triangle)$ (see Figure 47) on the set $\{A, B, C, D\}$ of modified triangles shown below.

**Figure 45** $S(\square)$ **Figure 46** The lines of symmetry of the square**Figure 47** $S(\triangle)$

The Orbit–Stabiliser Theorem has the following immediate corollary.

Corollary E65

Suppose that the finite group G acts on the set X . Then, for each element x in X , the number of elements in $\text{Orb } x$ divides the order of G .

For example, the orbits in the table in the solution to Exercise E165 have 4, 8, 2 and 1 elements, respectively, and these numbers all divide 8, the order of $S(\square)$.

Of course, it also follows from the Orbit–Stabiliser Theorem that if a finite group G acts on a set X , then for each element x in X the number of elements in $\text{Stab } x$ divides the order of G . However, we knew that already: it follows from Lagrange’s Theorem, since $\text{Stab } x$ is a subgroup of G .

3.2 Left cosets of stabilisers

Since the stabiliser of a set element under a group action is a subgroup of the group that is acting, it has cosets in this group. In this subsection you will meet an important property of the *left* cosets of stabilisers. We will use this property to prove the Orbit–Stabiliser Theorem.

You might wonder why the property involves left cosets and not right cosets. This is because of the way that we defined a group action. The concept that we have been calling a group action is more accurately called a *left group action*.

In the definition of a group action that you met earlier, axiom GA3 is as follows:

GA3 Composition For all $g, h \in G$ and all $x \in X$,

$$g \wedge (h \wedge x) = (g \circ h) \wedge x.$$

If we replace axiom GA3 with the following alternative axiom, then we obtain the definition of a *right group action*:

GA3 Composition (different) For all $g, h \in G$ and all $x \in X$,

$$g \wedge (h \wedge x) = (h \circ g) \wedge x.$$

If we had used this alternative definition, then we would have obtained a theory analogous to the one developed in this unit, just with a few things ‘the other way round’. The situation is similar to that for left and right cosets. We will continue to use our original axiom GA3 throughout this unit – that is, we will continue to work with left group actions, and call them simply group actions.

Here is an example that illustrates the property of left cosets of stabilisers introduced in this subsection. Consider the action of the group $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 48), and consider in particular the vertex label 1.

The elements of $S(\square)$ that fix 1 are e and s , so

$$\text{Stab } 1 = \{e, s\}.$$

We will now find the left cosets of $\text{Stab } 1$ in $S(\square)$. Using our usual method for finding cosets and referring to Table 1, we find that they are

$$\begin{aligned} \text{Stab } 1 &= \{e, s\}, \\ a \text{ Stab } 1 &= \{a \circ e, a \circ s\} = \{a, t\}, \\ b \text{ Stab } 1 &= \{b \circ e, b \circ s\} = \{b, u\}, \\ c \text{ Stab } 1 &= \{c \circ e, c \circ s\} = \{c, r\}. \end{aligned}$$

Now let us partition $S(\square)$ in another way, namely according to where its elements map the vertex label 1. We can see from Figure 48 that

$$\begin{aligned} e \text{ and } s &\text{ map } 1 \text{ to } 1 \text{ (of course, since } e, s \in \text{Stab } 1), \\ a \text{ and } t &\text{ map } 1 \text{ to } 2, \\ b \text{ and } u &\text{ map } 1 \text{ to } 3, \\ c \text{ and } r &\text{ map } 1 \text{ to } 4. \end{aligned}$$

So the partition of $S(\square)$ according to where its elements map 1 is

$$\{e, s\}, \quad \{a, t\}, \quad \{b, u\}, \quad \{c, r\}.$$

This is the same as the partition of $S(\square)$ into left cosets of $\text{Stab } 1$.

So if two elements of $S(\square)$ lie in the *same* left coset of $\text{Stab } 1$, then they map 1 to the *same* vertex label, whereas if they lie in *different* left cosets, then they map 1 to *different* vertex labels.

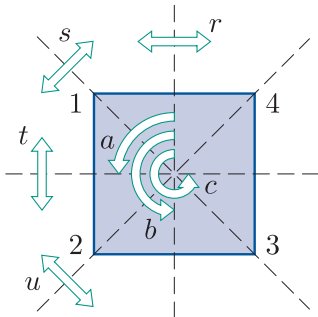


Figure 48 $S(\square)$

Table 1 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

In the next exercise you are asked to determine whether a similar property holds for the vertex label 2 under the same group action.

Exercise E167

Consider the action of the group $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 49).

- Find $\text{Stab } 2$.
- Find the left cosets of $\text{Stab } 2$ in $S(\square)$. (The group table of $S(\square)$ is given as Table 2.)
- Partition $S(\square)$ according to where its elements map the vertex label 2.
- Are the partitions that you found in parts (b) and (c) the same?

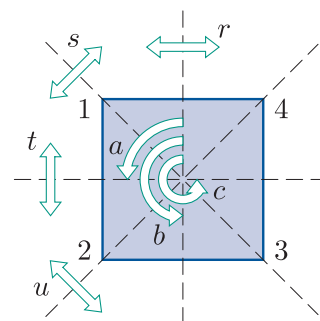


Figure 49 $S(\square)$

Table 2 $S(\square)$

| \circ | e | a | b | c | r | s | t | u |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|
| e | e | a | b | c | r | s | t | u |
| a | a | b | c | e | s | t | u | r |
| b | b | c | e | a | t | u | r | s |
| c | c | e | a | b | u | r | s | t |
| r | r | u | t | s | e | c | b | a |
| s | s | r | u | t | a | e | c | b |
| t | t | s | r | u | b | a | e | c |
| u | u | t | s | r | c | b | a | e |

The examples above are instances of the following general result, which is illustrated in Figure 50.

Theorem E66

Let \wedge be an action of a group (G, \circ) on a set X , let x be an element of X and let g and h be elements of G . Then

$$g \wedge x = h \wedge x$$

if and only if

g and h lie in the same left coset of $\text{Stab } x$.

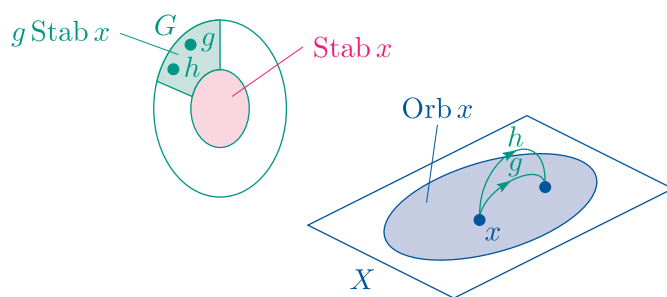


Figure 50 Group elements g and h map set element x to the same element if and only if they lie in the same left coset of $\text{Stab } x$

Proof of Theorem E66 ‘If’ part

Suppose that g and h lie in the same left coset of $\text{Stab } x$. Then $h \in g \text{Stab } x$, so $h = g \circ k$ for some $k \in \text{Stab } x$. It follows that

$$\begin{aligned} h \wedge x &= (g \circ k) \wedge x \\ &= g \wedge (k \wedge x) \quad (\text{by axiom GA3}) \\ &= g \wedge x \quad (\text{since } k \in \text{Stab } x), \end{aligned}$$

as required.

‘Only if’ part

Suppose that

$$g \wedge x = h \wedge x.$$

Consider the effect of the group element $g^{-1} \circ h$ on x :

$$\begin{aligned} (g^{-1} \circ h) \wedge x &= g^{-1} \wedge (h \wedge x) && \text{(by axiom GA3)} \\ &= g^{-1} \wedge (g \wedge x) && \text{(since } g \wedge x = h \wedge x) \\ &= (g^{-1} \circ g) \wedge x && \text{(by axiom GA3)} \\ &= e \wedge x \\ &= x && \text{(by axiom GA2).} \end{aligned}$$

Therefore $g^{-1} \circ h = k$ for some $k \in \text{Stab } x$. It follows, by composing each side of this equation on the left by g , that $h = g \circ k$. Hence $h \in g \text{ Stab } x$. Thus g and h lie in the same left coset of $\text{Stab } x$. ■

Theorem E66 tells us that if a group G acts on a set X and x is any element of X , then the sets of group elements that map x to the same element of X are precisely the left cosets of $\text{Stab } x$. This means that

if we collect together the group elements according to where they map x , then we have the left cosets of $\text{Stab } x$,

and that, conversely,

if we find the left cosets of $\text{Stab } x$, then we have the sets of group elements that map x to the same element of X .

In the next exercise you are asked to check Theorem E66 for a set element under another group action.

Exercise E168

Consider the action of the symmetric group S_3 on the set $\{1, 2, 3\}$ of symbols.

- (a) Find $\text{Stab } 1$.
- (b) Find the left cosets of $\text{Stab } 1$.
- (c) Partition S_3 according to where its elements map the symbol 1.
- (d) Check whether the partitions that you found in parts (b) and (c) are the same.

Although the examples illustrating Theorem E66 that you have seen so far all involve actions of finite groups on finite sets, the theorem applies to *all* group actions, no matter whether the group and set involved are finite or infinite.

We can now use Theorem E66 to prove the Orbit–Stabiliser Theorem. The proof is based on the following idea. Consider any action of a group G on a set X , and let x be an element of X . By Theorem E66, the sets of elements of G that map x to the same element are precisely the left cosets of $\text{Stab } x$ in G . It follows that we can define a mapping, say f , whose domain is the set of left cosets of $\text{Stab } x$ in G , whose codomain is $\text{Orb } x$, and whose rule is

left coset \mapsto element of $\text{Orb } x$ to which each element of the left coset maps x .

This mapping f is illustrated in Figure 51.

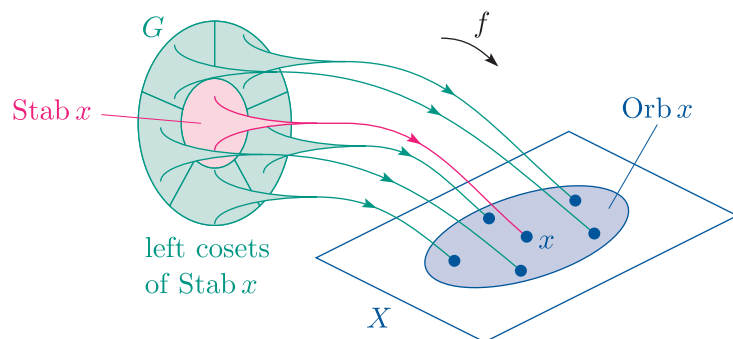


Figure 51 The mapping f obtained from the stabiliser of an element x

For example, consider again the action of the group $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square, and the particular vertex label 1.

Near the start of this subsection you saw that under this group action the left cosets of $\text{Stab } 1$ are

$$\{e, s\}, \quad \{a, t\}, \quad \{b, u\}, \quad \{c, r\}.$$

You also saw that

both elements of the left coset $\{e, s\}$ ($\text{Stab } 1$ itself) map 1 to 1,
both elements of the left coset $\{a, t\}$ map 1 to 2,
both elements of the left coset $\{b, u\}$ map 1 to 3,
both elements of the left coset $\{c, r\}$ map 1 to 4.

So the mapping f obtained from $\text{Stab } 1$ as described above is

$$\begin{aligned} f : \text{set of left cosets of } \text{Stab } 1 &\longrightarrow \text{Orb } 1 \\ \{e, s\} &\mapsto 1 \\ \{a, t\} &\mapsto 2 \\ \{b, u\} &\mapsto 3 \\ \{c, r\} &\mapsto 4 \end{aligned}$$

This mapping f is illustrated in Figure 52.

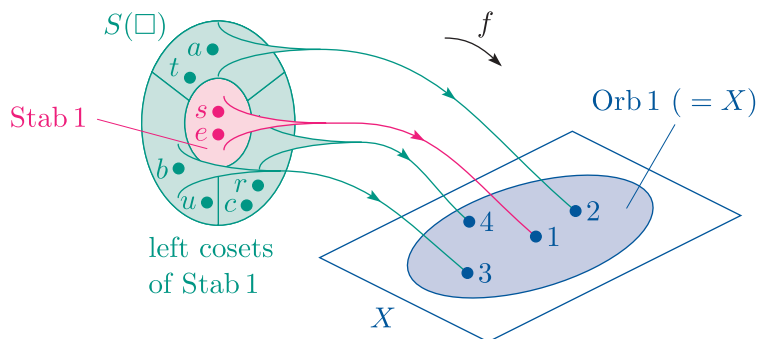


Figure 52 The mapping f obtained from $\text{Stab } 1$ under the action of $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square

In this example the orbit of the set element considered, $\text{Orb } 1$, is the whole of the set X on which the group acts, but in other examples the orbit may be a proper subset of X .

Exercise E169

Consider again the action of the group $S(\square)$ on the set of vertex labels of the square (see Figure 53). By referring to your solution to Exercise E167, write down the mapping f obtained from $\text{Stab } 2$ in the way described above.

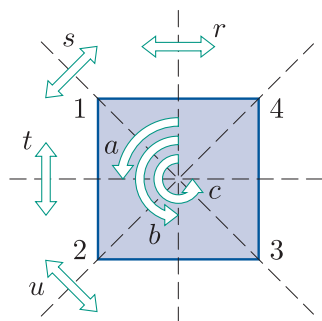


Figure 53 $S(\square)$

The mapping f obtained from the stabiliser of a set element under a group action in the way described above is always one-to-one and onto, just because of how it is defined. This fact is stated formally in the following corollary to Theorem E66. It is the key to proving the Orbit–Stabiliser Theorem, as you will see shortly.

Corollary E67

Let \wedge be an action of a group G on a set X and let x be an element of X . Then the mapping f given by

$$f : \text{set of left cosets of } \text{Stab } x \longrightarrow \text{Orb } x$$

$$g \text{Stab } x \longmapsto g \wedge x$$

is one-to-one and onto.

Proof The mapping f defined above maps each left coset of $\text{Stab } x$ to $g \wedge x$, where g is any element of the left coset. This is a valid definition of a mapping because, by Theorem E66, $g \wedge x$ is the *same* element of X for *every* group element g in any particular left coset of $\text{Stab } x$.

Theorem E66 tells us that elements from *different* left cosets of $\text{Stab } x$ map x to *different* elements of X , so f is one-to-one.

Also, f is onto, because each element $g \wedge x$ of $\text{Orb } x$ is the image under f of the left coset $g \text{Stab } x$. ■

We now use Corollary E67 to prove the Orbit–Stabiliser Theorem. Unlike Theorem E66 and Corollary E67, the Orbit–Stabiliser Theorem is a result about *finite* groups only.

Theorem E64 Orbit–Stabiliser Theorem

Suppose that the finite group G acts on the set X . Then, for each element x in X ,

$$|\text{Orb } x| \times |\text{Stab } x| = |G|.$$

Proof Let x be an element of X . Corollary E67 tells us that the left cosets of $\text{Stab } x$ can be matched one-to-one with the elements of $\text{Orb } x$. Hence the number of left cosets of $\text{Stab } x$ is the same as the number of elements in $\text{Orb } x$. But the number of left cosets of $\text{Stab } x$ is equal to $|G|/|\text{Stab } x|$, so

$$|G|/|\text{Stab } x| = |\text{Orb } x|,$$

and hence

$$|\text{Orb } x| \times |\text{Stab } x| = |G|. \quad \blacksquare$$

3.3 Groups acting on groups

In this subsection we will look at some examples of actions of a group G on a set X where X is itself a group. Often, but not always, the set X is the group G itself. Such actions have important applications in group theory, as you will see.

Throughout the subsection we will mostly use concise multiplicative notation for abstract groups: that is, we will not use symbols for their binary operations. This is convenient when we have to deal with many composites of group elements, as you have seen before.

The definition of a group action is translated into concise multiplicative notation below. There are only two differences: we refer to the group as G instead of (G, \circ) , and in axiom GA3 we write $(gh) \wedge x$ instead of $(g \circ h) \wedge x$.

Definition

Let G be a group with identity element e , and let X be a set. Suppose that for each element g in G and each element x in X an object $g \wedge x$ is defined in some way.

We say that the effect \wedge of G on X is a **group action** of G on X , or simply an **action** of G on X , and that G **acts on** X , if the following three axioms hold.

GA1 Closure For each $g \in G$ and each $x \in X$,

$$g \wedge x \in X.$$

GA2 Identity For each $x \in X$,

$$e \wedge x = x.$$

GA3 Composition For all $g, h \in G$ and all $x \in X$,

$$g \wedge (h \wedge x) = (gh) \wedge x.$$

The first action of a group on a group that we consider in this subsection is *conjugation*. The proposition below shows that conjugation is an action of a group on itself.

Proposition E68

Let G be a group, and let \wedge be defined by

$$g \wedge x = gxg^{-1}$$

for all $g, x \in G$. Then \wedge is an action of G on itself.

Proof We show that the group action axioms hold.

GA1 Closure Let $g, x \in G$. Then

$$g \wedge x = gxg^{-1} \in G.$$

Thus axiom GA1 holds.

GA2 Identity Let e be the identity element of G and let $x \in G$. Then

$$e \wedge x = exe^{-1} = x.$$

Thus axiom GA2 holds.

GA3 Composition Let $g, h, x \in G$. We have to check that

$$g \wedge (h \wedge x) = (gh) \wedge x.$$

Now

$$\begin{aligned}
 g \wedge (h \wedge x) &= g \wedge (h x h^{-1}) \\
 &= g h x h^{-1} g^{-1} \\
 &= (gh)x(gh)^{-1} \quad (\text{since } h^{-1}g^{-1} = (gh)^{-1}) \\
 &= (gh) \wedge x.
 \end{aligned}$$

Thus axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action. ■

Exercise E170

Let G be a group. Determine which of the following define a group action \wedge of G on itself.

- (a) $g \wedge x = gx$ for all $g, x \in G$.
- (b) $g \wedge x = xg$ for all $g, x \in G$.
- (c) $g \wedge x = xg^{-1}$ for all $g, x \in G$.

We will now revisit some topics in group theory in the light of group actions.

Lagrange's Theorem

Lagrange's Theorem is related to the group action defined in the exercise below, as you will see. This group action is slightly different from those that you have met so far in this section: it does not necessarily involve an action of a group on itself, but instead involves an action of a *subgroup* on the group.

Exercise E171

Let H be a subgroup of a group G . Let \wedge be defined by

$$h \wedge g = hg$$

for all $h \in H$ and all $g \in G$. Show that \wedge defines an action of H on G .

Now let H be a subgroup of a group G , and consider the action of H on G defined in Exercise E171. Let us investigate its orbits. For any element g of G ,

$$\text{Orb } g = \{h \wedge g : h \in H\} = \{hg : h \in H\}.$$

This is just the right coset Hg . So the orbits of this group action are precisely the *right cosets of H in G* . Hence the partition of a group G into the right cosets of a subgroup H is a particular instance of the partition of a group into the orbits of a group action.

Now suppose that the group G is finite. Corollary E65, an immediate corollary of the Orbit–Stabiliser Theorem, states that the number of elements in an orbit of an action of a finite group divides the order of the group. Applying this result to the group action above tells us that the number of elements in each right coset of H in G divides the order of G . Since H is one of the right cosets, this tells us that the order of H divides the order of G . This is Lagrange’s Theorem, so Lagrange’s Theorem is a special case of Corollary E65.

Conjugacy classes

We will now use group actions to prove a theorem about *conjugacy classes* that was stated but not proved in Unit E2 *Quotient groups and conjugacy*.

You saw in Unit E2 that every group splits into conjugacy classes: elements in the same conjugacy class are conjugate to each other in the group, and elements in different classes are not conjugate to each other in the group.

For example, the conjugacy classes of the symmetry group $S(\triangle)$ (see Figure 54) are as follows (they were found in Exercise E77 in Subsection 2.3 of Unit E2):

| | |
|---------------|---|
| $\{e\}$ | identity |
| $\{a, b\}$ | anticlockwise and clockwise rotations through $2\pi/3$ |
| $\{r, s, t\}$ | reflections in lines through vertices and midpoints of edges. |

You met the following theorem in Subsection 2.3 of Unit E2.

Theorem E27

In any finite group G , the number of elements in each conjugacy class divides the order of G .

For instance, the numbers of elements in the conjugacy classes of $S(\triangle)$ are 1, 2 and 3, respectively, and each of these numbers divides 6, the order of $S(\triangle)$.

We can now use the group action defined in Proposition E68 earlier in this subsection to prove Theorem E27.

Proof of Theorem E27 Let G be a finite group, and let \wedge be defined by

$$g \wedge x = gxg^{-1}$$

for all $g, x \in G$. By Proposition E68, \wedge is an action of G on itself.

For any element x in G , the orbit of x under \wedge is

$$\begin{aligned} \text{Orb } x &= \{g \wedge x : g \in G\} \\ &= \{gxg^{-1} : g \in G\}. \end{aligned}$$

This is the conjugacy class of G containing x .

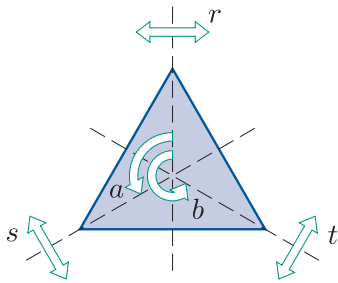


Figure 54 $S(\triangle)$

Thus the orbits of this group action are precisely the conjugacy classes of G . By Corollary E65 to the Orbit–Stabiliser Theorem, the number of elements in each orbit divides the order of G , which proves the result. ■

Homomorphisms

We can also recognise a result about homomorphisms from Unit E3 as a special case of the Orbit–Stabiliser Theorem. To do this, we apply the Orbit–Stabiliser Theorem to the group action in the next exercise.

Exercise E172

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Let \wedge be defined by

$$g \wedge h = \phi(g) * h,$$

for all $g \in G$ and $h \in H$. (Notice that it is the binary operation of the group $(H, *)$ that is used in the definition of \wedge .)

Show that \wedge is an action of the group (G, \circ) on the group $(H, *)$.

Now let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism where (G, \circ) is a *finite* group, and let \wedge be the action of (G, \circ) on $(H, *)$ defined in Exercise E172.

Let us find the orbit and stabiliser of e_H , the identity element of $(H, *)$, under this group action.

The orbit of e_H is

$$\begin{aligned} \text{Orb } e_H &= \{g \wedge e_H : g \in G\} \\ &= \{\phi(g) * e_H : g \in G\} \\ &= \{\phi(g) : g \in G\}. \end{aligned}$$

This set is the *image* of ϕ . So $\text{Orb } e_H = \text{Im } \phi$.

The stabiliser of e_H is

$$\begin{aligned} \text{Stab } e_H &= \{g \in G : g \wedge e_H = e_H\} \\ &= \{g \in G : \phi(g) * e_H = e_H\} \\ &= \{g \in G : \phi(g) = e_H\}. \end{aligned}$$

This set is the *kernel* of ϕ . So $\text{Stab } e_H = \text{Ker } \phi$.

By the Orbit–Stabiliser Theorem,

$$|\text{Orb } e_H| \times |\text{Stab } e_H| = |G|.$$

Therefore

$$|\text{Im } \phi| \times |\text{Ker } \phi| = |G|.$$

This is Corollary E56 from Unit E3 – it is a corollary of the First Isomorphism Theorem. Thus Corollary E56 is a special case of the Orbit–Stabiliser Theorem.

Group actions can be used to prove many other results in group theory. The examples that you have seen in this subsection illustrate the power of this approach.

4 The Counting Theorem

A **counting problem** is a problem that asks how many objects there are of a particular type. In this section you will learn how to solve some counting problems that involve symmetry. Many problems of this kind look hard to answer at first sight, but become much more straightforward if we apply ideas relating to group actions.

4.1 Counting problems involving symmetry

Some simple counting problems are easily solved by using the following rule.

Multiplication Principle

If we have k successive choices to make, and the i th choice involves choosing from n_i options, for each $i = 1, 2, \dots, k$, then the total number of ways to make all k choices is

$$n_1 \times n_2 \times \cdots \times n_k.$$

Here is an example.

Worked Exercise E71

How many distinct sequences of two coloured discs are there in which each disc is coloured blue, yellow or red? Some examples of such sequences are shown below.



Solution

There are three choices of colour for the first disc and three choices of colour for the second disc, so by the Multiplication Principle the number of such sequences is

$$3 \times 3 = 9.$$

The nine sequences from Worked Exercise E71 are shown in Figure 55.

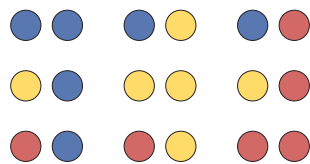


Figure 55 The different sequences of two discs coloured blue, yellow or red

Exercise E173

A 2×2 pattern of plain coloured tiles is to be mounted on a wall. How many different patterns are possible if tiles are available in blue, yellow, red, green and purple? Some examples of such patterns are shown below.



Now consider the following counting problem.

Bangle problem How many different bangles decorated with six equally spaced beads can be made if beads are available in blue, yellow and red? Some examples of such bangles are shown in Figure 56.



Figure 56 Six-bead bangles made using blue, yellow and red beads

If the bangles in this problem cannot be rotated or turned over – that is, if their positions are fixed – then we can answer this question by using the Multiplication Principle. There are six beads, and each of them can be any of the three colours, so the number of different bangles is

$$3 \times 3 \times 3 \times 3 \times 3 \times 3 = 3^6 = 729.$$

However, such a bangle *can* be rotated or turned over, of course. For example, we would regard the two bangles in Figure 57 as the same, since either can be rotated to give the other.

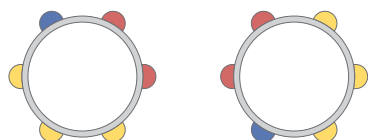


Figure 57 Two bangles each of which can be rotated to give the other

Similarly, we would regard the two bangles in Figure 58 as the same, since either can be turned over to give the other.

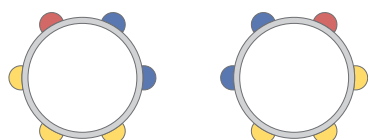
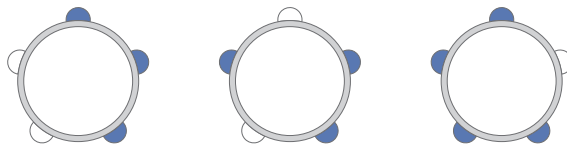


Figure 58 Two bangles each of which can be turned over to give the other

The symmetry of the objects involved in this counting problem makes it much more difficult to solve than the problems in Worked Exercise E71 and Exercise E173.

Exercise E174

Consider the problem of finding the number of different bangles that can be made using *five* equally spaced beads, if beads are available in just *two* colours, blue and white. Some examples of such bangles are shown below.



- How many different bangles are there if the bangles cannot be rotated or turned over?
- By drawing all the possibilities, find the number of different bangles if two bangles are regarded as the same whenever one can be rotated or turned over to give the other.

What has all this got to do with group actions? To see this, consider again the original bangle problem above, which concerned six-bead bangles made using beads available in three colours. Let X be the set of all 3^6 coloured bangles in fixed positions. We can think of the beads on each bangle as being placed at the vertices of a regular hexagon, and we can think of turning a bangle over as reflecting it, so the symmetry group of the bangle (when we ignore the colours of the beads) is essentially the symmetry group $S(\hexagon)$ of the regular hexagon. The rotations and reflections in $S(\hexagon)$ map bangles in X to other bangles in X , and the effect of $S(\hexagon)$ on X is a group action by Theorem E60.

We want to regard two bangles in the set X as the same if either can be rotated or reflected to give the other. In other words, we want to regard two bangles as the same if they *lie in the same orbit* of the action of the group $S(\hexagon)$ on the set X . Thus the bangle problem can be rephrased as follows.

Let X be the set of all possible bangles in fixed positions decorated with six equally spaced beads each coloured blue, yellow or red. How many orbits are there in the action of the group $S(\hexagon)$ on the set X ?

Later in this section you will meet a theorem, the *Counting Theorem*, that gives a formula for the number of orbits of an action of a finite group on a finite set. You will see how to use it to answer counting problems such as the one above.

First, however, we will look at a few more counting problems that illustrate the kinds of questions that we can answer by using the Counting Theorem. Here is another example of such a problem.

Chessboard problem How many different patterns can be made by colouring the squares of a chessboard either black or white?

If the chessboard in this problem is fixed in place – for example, if it is displayed on a wall – then we can answer this question by using the

Multiplication Principle, as follows. A chessboard has 64 squares and each square can be coloured with either of two colours, so the total number of coloured chessboards is

$$\underbrace{2 \times 2 \times 2 \times \cdots \times 2}_{64 \text{ copies of } 2} = 2^{64}.$$

However, usually a chessboard can be rotated, so we would want to regard two coloured chessboards as the same if one can be rotated to give the other. For example, we would want to regard the two coloured chessboards in Figure 59 as the same, as a quarter turn anticlockwise turns the first into the second. A chessboard usually appears on only one side of its board, so we would *not* want to regard two coloured chessboards as the same if one can be reflected to give the other (except in cases where one can also be rotated to give the other, of course).

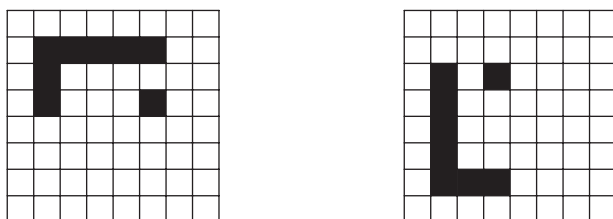


Figure 59 Two coloured chessboards each of which can be rotated to give the other

In the next exercise you are asked to look at a similar but smaller problem.

Exercise E175

There are $2^4 = 16$ ways of colouring the squares of a 2×2 chessboard in a fixed position either black or white (by the Multiplication Principle).

Three of them are shown below.



- Draw all 16 coloured chessboards in fixed positions.
- By using your drawings, determine how many different such coloured chessboards there are when we regard two of them as the same if one can be rotated to give the other.

Like the bangle problem, the chessboard problem can be interpreted in terms of a group action. Let X be the set of all 2^{64} coloured chessboards in fixed positions. We want to regard two coloured chessboards as the same when one can be rotated to give the other, so we consider the action of the group $S^+(\square)$ of rotations of the square on the set X . Then we are regarding two coloured chessboards as the same when they belong to the same orbit of this group action, so the answer to the chessboard problem is the number of orbits of the group action.

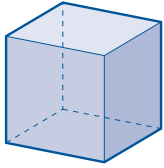


Figure 60 A cube

Finally consider the following counting problem.

Cube problem How many different coloured cubes are there with each face painted one of blue, yellow or red?

A cube (see Figure 60) has six faces, and in this problem each of them is to be coloured with one of three colours, so by the Multiplication Principle there are 3^6 coloured cubes in fixed positions. However, we would want to regard two coloured cubes as the same when one can be rotated to give the other.

We can interpret this problem in terms of a group action as follows. We let X be the set of all 3^6 coloured cubes in fixed positions. We want to regard two coloured cubes as the same when one can be rotated to give the other, so we consider the action of the group $S^+(\text{cube})$ of rotations of the cube on the set X . Then we are regarding two coloured cubes as the same when they belong to the same orbit of this group action, so the answer to the cube problem is the number of orbits of the group action.

There is one more concept relating to group actions that you need to learn about before you can meet the Counting Theorem and discover how to solve problems such as those in this subsection. This is the concept of *fixed sets*, which is covered in the next subsection.

4.2 Fixed sets

We make the following definition.

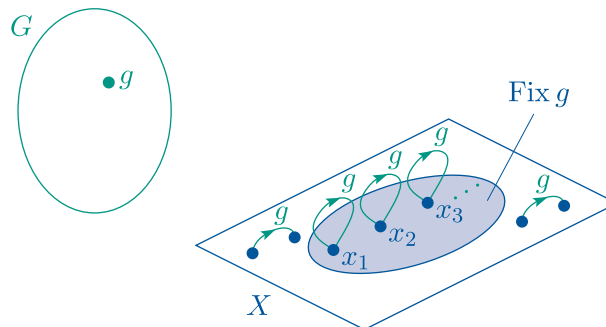
Definition

Let \wedge be an action of a group G on a set X , and let g be an element of G . The **fixed set** of g under \wedge , denoted by $\text{Fix } g$, is given by

$$\text{Fix } g = \{x \in X : g \wedge x = x\}.$$

That is, $\text{Fix } g$ is the set of elements of X that are fixed by g .

This definition is illustrated in Figure 61.

Figure 61 The fixed set of a group element g

Notice that it is an element of the *group* G , not an element of the *set* X , that has a fixed set. This is in contrast to orbits and stabilisers, each of which is a set associated with an element of the set X . Fixed sets, like stabilisers, are concerned with elements of the group G fixing elements of the set X , but from the opposite point of view:

- the fixed set of an element g in G is the set of all elements of X that are fixed by g
- the stabiliser of an element x in X is the set of all elements of G that fix x .

In particular, $\text{Fix } g$ is a subset of X , whereas $\text{Stab } x$ is a subgroup of G .

The fixed set of the identity element e of the group G is always the whole set X , since by axiom GA2 the identity element e fixes every element of X .

Worked Exercise E72

Consider the action of the group $S(\square)$ (see Figure 62) on the set $\{R, S, T, U\}$ of lines of symmetry of the square (see Figure 63). Write down the fixed set of each element of $S(\square)$ under this group action.

Solution

To find $\text{Fix } r$, for example, we consider the effect of the transformation r on each element of $\{R, S, T, U\}$:

$$\begin{aligned} r \wedge R &= R, \\ r \wedge S &= U, \\ r \wedge T &= T, \\ r \wedge U &= S. \end{aligned}$$

The elements of $\{R, S, T, U\}$ that are fixed by r are R and T , so $\text{Fix } r = \{R, T\}$. We find the fixed sets of the other elements of $S(\square)$ in a similar way.

The fixed sets are

$$\begin{aligned} \text{Fix } e &= \{R, S, T, U\}, \\ \text{Fix } a &= \emptyset \quad (\text{the empty set}), \\ \text{Fix } b &= \{R, S, T, U\}, \\ \text{Fix } c &= \emptyset, \\ \text{Fix } r &= \{R, T\}, \\ \text{Fix } s &= \{S, U\}, \\ \text{Fix } t &= \{R, T\}, \\ \text{Fix } u &= \{S, U\}. \end{aligned}$$

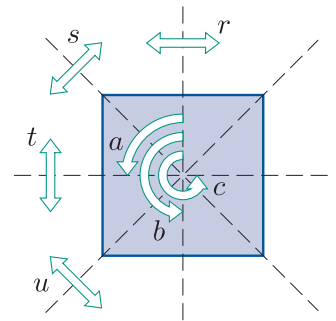


Figure 62 $S(\square)$

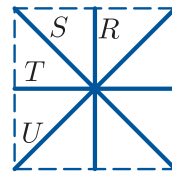
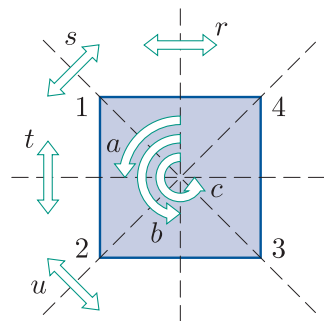
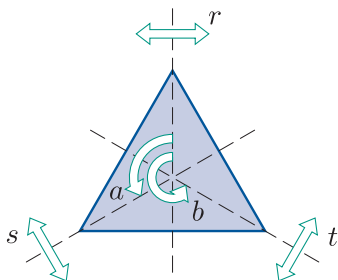
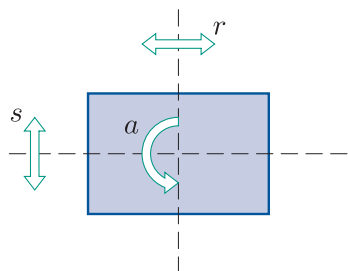


Figure 63 The lines of symmetry of the square

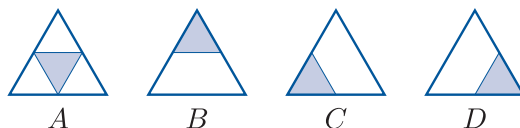
Figure 64 $S(\square)$ Figure 65 $S(\triangle)$ Figure 66 $S(\square)$

Exercise E176

Write down the fixed set of each element of the group $S(\square)$ under the action of $S(\square)$ on the set $\{1, 2, 3, 4\}$ of vertex labels of the square (see Figure 64).

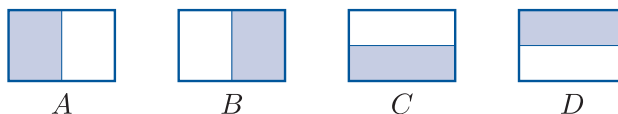
Exercise E177

Write down the fixed set of each element of the group $S(\triangle)$ (see Figure 65) under the action of $S(\triangle)$ on the set $\{A, B, C, D\}$ of modified triangles shown below.



Exercise E178

Write down the fixed set of each element of the group $S(\square)$ (see Figure 66) under the action of $S(\square)$ on the set $\{A, B, C, D\}$ of modified rectangles shown below.



The fixed point sets that you met in Subsection 4.1 of Unit E2 are special cases of fixed sets. You saw there that if f is a symmetry of a figure F , then the *fixed point set* of f is the set of all points of F that are fixed by f . This is the fixed set of f under the natural action of the symmetry group $S(F)$ on the set of points in F .

The next worked exercise and the exercise that follows involve finding fixed sets under the action of a group on the plane \mathbb{R}^2 .

Worked Exercise E73

Let

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R}^+ \right\}.$$

Consider the action of the group (G, \times) on the set \mathbb{R}^2 defined by

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \wedge (x, y) = (ax, by)$$

for all $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$.

(This is the same group action as in Worked Exercise E64 in Subsection 2.2 and Worked Exercise E69 in Subsection 2.4.)

- (a) Find an expression for the fixed set of a general element of the group (G, \times) under this group action.
- (b) Find the fixed set of each of the following elements of (G, \times) under the group action. Describe each fixed set geometrically.


(i) $\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Solution

- (a)  We have to apply the general definition of a fixed set,

$$\text{Fix } g = \{x \in X : g \wedge x = x\},$$

to the situation here. We

- replace g by a general element of the group G , say $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$
- replace x by a general element of the set \mathbb{R}^2 , say (x, y) . 



For any matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G$ (so $a, b \in \mathbb{R}^+$),

$$\begin{aligned} \text{Fix } \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} &= \left\{ (x, y) \in \mathbb{R}^2 : \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \wedge (x, y) = (x, y) \right\} \\ &= \{ (x, y) \in \mathbb{R}^2 : (ax, by) = (x, y) \} \\ &= \{ (x, y) \in \mathbb{R}^2 : ax = x \text{ and } by = y \}. \end{aligned}$$

- (b) (i) By part (a),

$$\begin{aligned} \text{Fix } \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} &= \{ (x, y) \in \mathbb{R}^2 : 1x = x \text{ and } 3y = y \} \\ &= \{ (x, y) \in \mathbb{R}^2 : y = 0 \} \\ &= \{ (x, 0) : x \in \mathbb{R} \}. \end{aligned}$$

So this fixed set is the x -axis.

- (ii)  Here the given matrix is the identity element of (G, \times) . Under any group action the identity element of the group fixes every element of the set, by axiom GA2. So there is no need to use the formula from part (a) here (though of course it would give the same answer). 

Since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of G ,

$$\text{Fix } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{R}^2.$$

That is, this fixed set is the whole plane \mathbb{R}^2 .

Exercise E179

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Consider the action of the group (G, \times) on the set \mathbb{R}^2 defined by

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (ax, y)$$

for all $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ and all $(x, y) \in \mathbb{R}^2$. (You saw that this is a group action in Exercise E143(a) in Subsection 1.4.)

- Find an expression for the fixed set of a general element of the group (G, \times) under this group action.
- Find the fixed set of each of the following elements of (G, \times) under the group action. Describe each fixed set geometrically.

$$(i) \begin{pmatrix} -1 & 5 \\ 0 & 1 \end{pmatrix} \quad (ii) \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

You will need to use the idea of fixed sets in the next subsection, where you will meet the Counting Theorem and see how to use it to solve counting problems involving symmetry. Using the Counting Theorem in this way usually involves considering the action of a finite group G of symmetries on a large finite set X of coloured figures. To be able to apply the Counting Theorem we need to know the *sizes* of the fixed sets of the elements of G , that is, the numbers of elements that the fixed sets contain. So we will now look at how we can find the sizes of fixed sets in this sort of situation. Here is an example.

Worked Exercise E74

Consider the action of the group $S(\triangle)$ (see Figure 67) on the set X whose elements are all the coloured figures obtained by colouring each of the four small triangles in the figure on the left below with one of the three colours blue, yellow and red. Some examples of elements of the set X are shown on the right below.

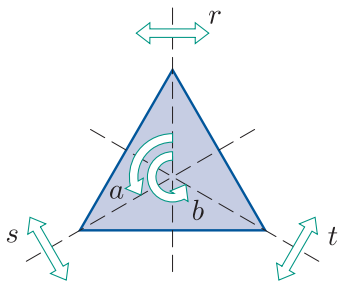


Figure 67 $S(\triangle)$



Find the size of $\text{Fix } g$ for each symmetry g in $S(\triangle)$.

Solution

☁ We consider each symmetry in $S(\triangle)$ in turn. ☁

- First consider the identity symmetry e . It fixes all the coloured figures in X .

There are four small triangles, each coloured with one of three colours, so the number of coloured figures in X is 3^4 (by the Multiplication Principle). Hence

$$|\text{Fix } e| = 3^4.$$

- Now consider the symmetry a .

☁ Let us think about the effect of a on some coloured figures in X . The symmetry a does not fix the first coloured figure below, because it maps it to the second coloured figure, which is different. However, it does fix the third coloured figure.



In general, we can say the following. ☁

The coloured figures in X fixed by the symmetry a are those in which the three outer triangles are all the same colour.

For such a coloured figure, there are three choices for the colour of the middle triangle and three choices for the single colour of the three outer triangles, so the number of such coloured figures is 3^2 . Hence

$$|\text{Fix } a| = 3^2.$$

By a similar argument,

$$|\text{Fix } b| = 3^2.$$

- Now consider the symmetry r .

☁ Let us think about the effect of r on some coloured figures in X . The symmetry r does not fix the first coloured figure below, because it maps it to the second coloured figure, which is different. However, it does fix the third coloured figure below.



In general, we can say the following. ☁

The coloured figures in X fixed by the symmetry r are those in which the bottom two outer triangles are the same colour.

For such a coloured figure there are three choices for the colour of the middle triangle, three choices for the colour of the top triangle, and three choices for the single colour of the bottom two outer triangles, so the number of such coloured figures is 3^3 . Hence

$$|\text{Fix } r| = 3^3.$$

By similar arguments,

$$|\text{Fix } s| = 3^3$$

and

$$|\text{Fix } t| = 3^3.$$

The sizes of the fixed sets for this group action are summarised below.

| Symmetry g | $ \text{Fix } g $ |
|--------------|-------------------|
| e | 3^4 |
| a | 3^2 |
| b | 3^2 |
| r | 3^3 |
| s | 3^3 |
| t | 3^3 |

In the solution to Worked Exercise E74, once we had found the size of $\text{Fix } a$, we could see that by a similar argument we would get the same answer for the size of $\text{Fix } b$. This is because the symmetries a and b are of the same geometric type. Similarly, once we had found the size of $\text{Fix } r$, we could see that by similar arguments we would get the same answers for the sizes of $\text{Fix } s$ and $\text{Fix } t$. Again this is because the symmetries r , s and t are of the same geometric type.

In fact, our observation that a and b are of the same geometric type is an observation that they are *conjugate* in $S(\triangle)$. You studied the connection between conjugacy and geometric type in symmetry groups in Subsection 4.1 of Unit E2: you saw there that two symmetries x and y of a figure F are conjugate in $S(F)$ if and only if there is a symmetry g of F that transforms a diagram illustrating x into a diagram illustrating y (when we ignore any labels).

In general, if a group G of symmetries of a figure F acts in the natural way on a set X of coloured figures, then symmetries in G that are conjugate in $S(F)$ have fixed sets of the same size (but usually not the same fixed sets).

In the solution to Worked Exercise E74, the sizes of the fixed sets were left as powers of the number of colours, rather than being evaluated. You should do likewise in the next exercise, and in the subsequent exercises in this subsection. This is convenient when we use the Counting Theorem, as you will see later.

Exercise E180

Consider the action of the group $S(\square)$ (see Figure 68) on the set X whose elements are all the coloured figures obtained by colouring each of the four small squares in the figure on the left below with one of the five colours blue, yellow, red, green and purple. Some examples of elements of X are shown on the right below.



Find the size of $\text{Fix } g$ for each symmetry g in $S(\square)$.

Exercise E181

Consider the group action that is the same as the one in Exercise E180 except that the figures in the set X are coloured with the *four* colours blue, yellow, red and green, instead of with five colours. By using your final answers to Exercise E180 and thinking about the arguments that you used to derive them, write down the size of $\text{Fix } g$ for each symmetry g in $S(\square)$. You should not need to work through all the arguments again.

The solution to Exercise E181 illustrates that if we have found the sizes of the fixed sets for the natural action of a group of symmetries on a set of coloured figures like those in the exercise and we want to change the number of colours, then it is straightforward to find the sizes of the resulting new fixed sets.

There is a method involving permutations that can help make finding the sizes of fixed sets like those in the last few exercises and worked exercises more systematic. It is based on considering the action of the group on the *set whose elements are the parts of the figure to be coloured*. For example, in Worked Exercise E74 the parts of the figure to be coloured are the four small triangles. The mapping effect of the group $S(\triangle)$ on these four triangles is a group action by Theorem E59.

The method is demonstrated in the next worked exercise, in which we look again at the question in Worked Exercise E74, but this time use the permutation method to carry out the working.

Worked Exercise E75

Consider the action of the group $S(\triangle)$ (see Figure 69 below) on the set X whose elements are all the coloured figures obtained by colouring each of the four small triangles in the figure below with one of the three colours blue, yellow and red.



Find the size of $\text{Fix } g$ for each symmetry g in $S(\triangle)$.

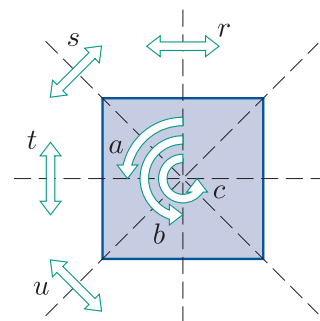


Figure 68 $S(\square)$

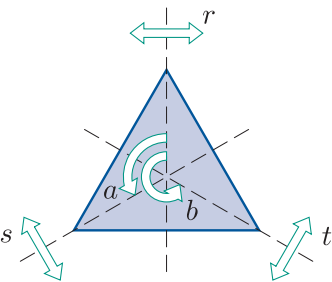
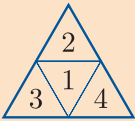


Figure 69 $S(\triangle)$

Solution

Label each part of the figure to be coloured with a symbol. Here we label the four small triangles.

We can label the figure as follows.



Express the effect of each symmetry on the parts to be coloured as a permutation, including any 1-cycles.

This gives the following.

| Symmetry g | Permutation |
|--------------|----------------|
| e | $(1)(2)(3)(4)$ |
| a | $(1)(2\ 3\ 4)$ |
| b | $(1)(2\ 4\ 3)$ |
| r | $(1)(2)(3\ 4)$ |
| s | $(1)(3)(2\ 4)$ |
| t | $(1)(4)(2\ 3)$ |

Consider the symmetry a , for example. It gives a permutation with two cycles: (1) and $(2\ 3\ 4)$. For a figure in X to be fixed by a , triangles in the same cycle must have the same colour, but triangles in different cycles can have different colours. Since there are three choices of colours for each cycle, the number of coloured figures fixed by a is 3^2 .

In general, by a similar argument, if the permutation given by a symmetry g has k cycles and there are c colours (here $c = 3$), then the number of coloured figures in X fixed by g is c^k .

So we can find the sizes of the fixed sets by adding to the table as follows.

| Symmetry g | Permutation | Number of cycles | $ \text{Fix } g $ |
|--------------|----------------|------------------|-------------------|
| e | $(1)(2)(3)(4)$ | 4 | 3^4 |
| a | $(1)(2\ 3\ 4)$ | 2 | 3^2 |
| b | $(1)(2\ 4\ 3)$ | 2 | 3^2 |
| r | $(1)(2)(3\ 4)$ | 3 | 3^3 |
| s | $(1)(3)(2\ 4)$ | 3 | 3^3 |
| t | $(1)(4)(2\ 3)$ | 3 | 3^3 |

Notice that, as you would expect, in the solution to Worked Exercise E75 symmetries of the same geometric type give permutations with the same cycle structure, leading to fixed sets of the same sizes.

Remember that when you use the method in Worked Exercise E75 it is *essential* to include 1-cycles.

In the next exercise you are asked to answer the question in Exercise E180 again, but this time using the method in Worked Exercise E75.

Here and in similar exercises the permutations that you obtain may be different from the ones given in the solution, because there are different ways to label the parts of the figure to be coloured. However, your permutations and the ones in the solutions should have the same cycle structures and hence the same numbers of cycles.

Exercise E182

As in Exercise E180, consider the action of the group $S(\square)$ (see Figure 70) on the set X whose elements are all the coloured figures obtained by colouring each of the four small squares in the figure below with one of the five colours blue, yellow, red, green and purple.



Use the method demonstrated in Worked Exercise E75 to find the size of $\text{Fix } g$ for each symmetry g in $S(\square)$.

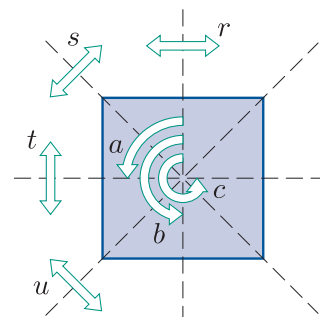


Figure 70 $S(\square)$

The permutation method introduced above will be useful in the next subsection.

4.3 The Counting Theorem and its use

In Subsection 4.1 you saw some examples of counting problems that can be interpreted as problems involving finding the number of orbits of an action of a finite group on a finite set. In this subsection you will meet the Counting Theorem and see how to use it to solve such counting problems.

The theorem is stated below. Its proof is given at the end of the subsection.

Theorem E69 Counting Theorem

Let \wedge be an action of a finite group G on a finite set X . Then the number of orbits of \wedge is given by

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix } g|.$$

The Counting Theorem tells us that one way to find the number of orbits of an action of a finite group G on a finite set X is to determine the number $|\text{Fix } g|$ for each element g in G , add up all these numbers, and divide the total by the order of G . Here is an example.

Worked Exercise E76

Use the Counting Theorem to determine how many different triangular window stickers similar to the one shown below can be made if each triangular region is to be coloured blue, yellow or red, and we regard two stickers as the same if one can be rotated or turned over to give the other.

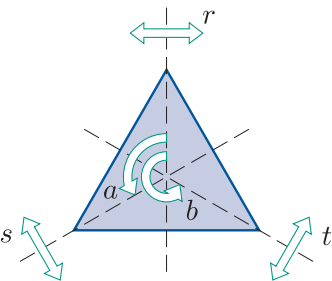


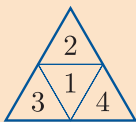
Figure 71 $S(\triangle)$

Solution

We want to regard two stickers as the same if one can be rotated or reflected to give the other, so we consider the action of the group $S(\triangle)$ (see Figure 71) on the set of all 3^4 coloured stickers in fixed positions.

The answer to the problem is the number of orbits of this group action, which we can find by using the Counting Theorem.

The sizes of the fixed sets for this group action were found in Worked Exercise E75 in the previous subsection, using the following labelled triangle.



The following table was obtained.

| Symmetry g | Permutation | Number of cycles | $ \text{Fix } g $ |
|--------------|----------------|------------------|-------------------|
| e | $(1)(2)(3)(4)$ | 4 | 3^4 |
| a | $(1)(2\ 3\ 4)$ | 2 | 3^2 |
| b | $(1)(2\ 4\ 3)$ | 2 | 3^2 |
| r | $(1)(2)(3\ 4)$ | 3 | 3^3 |
| s | $(1)(3)(2\ 4)$ | 3 | 3^3 |
| t | $(1)(4)(2\ 3)$ | 3 | 3^3 |

By the Counting Theorem, the number of orbits is

$$\begin{aligned}
 \frac{1}{6}(3^4 + 3^2 + 3^2 + 3^3 + 3^3 + 3^3) &= \frac{1}{6}(3^4 + 2 \times 3^2 + 3 \times 3^3) \\
 &= \frac{1}{6} \times 3^2(3^2 + 2 + 3^2) \\
 &= \frac{3}{2} \times 20 \\
 &= 30.
 \end{aligned}$$

Thus 30 different window stickers can be made.

So the Counting Theorem has reduced the complicated counting problem in Worked Exercise E76 to a straightforward calculation – such is the power of group theory!

Exercise E183

By using the Counting Theorem and your answers to Exercise E182 (or Exercise E180) in the previous subsection, determine how many different square headscarves, similar to the one shown below, can be made if each of the four square regions is to be coloured with one of the five colours blue, yellow, red, green and purple, and we regard two headscarves as the same if one can be rotated or turned over to give the other.



Exercise E184

Find the answer to Exercise E183 if each region of each headscarf is to be coloured with one of only *four* colours, instead of five colours.

Exercise E184 illustrates that if the number of colours in a counting problem of the type that we are considering is changed, then it is straightforward to adjust the solution accordingly.

The Counting Theorem is often incorrectly referred to as *Burnside's Lemma*. The British group theorist Peter M. Neumann (1940–) explained how this name arose in his 1979 paper *A lemma that is not Burnside's*.

It appears that the result was so well known in the early twentieth century that the British mathematician William Burnside (1852–1927) quoted it without attribution in the second (1911) edition of his classic book *Theory of Groups of Finite Order*. Fifty years later, it was misattributed to Burnside by the American mathematician Solomon Golomb (1932–2016) in a paper in 1961, following which the Dutch mathematician Nicolaas Govert de Bruijn (1918–2012) referred to it as ‘Burnside's lemma’ in papers in 1963 and 1964. The name was used subsequently by many other mathematicians. De Bruijn wrote to Neumann as follows:

Indeed, I think I am to blame, having used the name ‘Burnside's lemma’ in several of my papers. You describe correctly how this all went. Pólya did not give a reference, Golomb mentioned the name Burnside, I looked it up in Burnside's book and found it without reference, so that was that.

The result was known many years beforehand. It appears in a paper by the German mathematician Ferdinand Georg Frobenius (1849–1917) published in 1887, and earlier in a slightly different form in work of the French mathematician Augustin-Louis Cauchy (1789–1857) published in 1845. Neumann therefore suggested that a



Ferdinand Georg Frobenius



Augustin-Louis Cauchy

more appropriate name for it is the *Cauchy–Frobenius Lemma*. This name is now sometimes used, as are some other names such as the *Counting Theorem*, but despite Neumann’s paper being published only 18 years after the first misattribution of the result to Burnside in print, the name ‘Burnside’s lemma’ is still widely used.

(Source: Neumann, P. M. (1979) ‘A lemma that is not Burnside’s’, *Mathematical Scientist*, vol. 4, pp. 133–41.)

Exercise E185

Use the Counting Theorem to determine how many different 2×2 chessboards there are with each small square coloured either black or white, when we regard two chessboards as the same if one can be rotated to give the other. Hence check your answer to Exercise E175 in Subsection 4.1.

In the next worked exercise the bangle problem from Subsection 4.1 is solved using the Counting Theorem.

Worked Exercise E77

How many different bangles decorated with six equally spaced beads can be made if beads are available in blue, yellow and red? Some examples of such bangles are shown below.

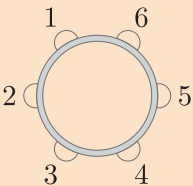


Solution

We are regarding two coloured bangles as the same if one can be rotated or turned over to give the other. So we consider the action of the group $S(\square)$ on the set of all possible coloured bangles in fixed positions.

There are six beads to be chosen and three choices for the colour of each bead, so there are 3^6 coloured bangles in fixed positions.

We can label the beads as shown below.



The sizes of the fixed sets for this group action are as given below.

For convenience, here we use the permutations of the beads to represent the symmetries in $S(\square)$, rather than using a different way of representing them in the first column of the table. We can do this because no two symmetries in $S(\square)$ give the same permutation of the beads.

| Symmetry g | Permutation | Number of cycles | $ \text{Fix } g $ |
|-----------------|--------------------|------------------|-------------------|
| e | (1)(2)(3)(4)(5)(6) | 6 | 3^6 |
| other rotations | (1 2 3 4 5 6) | 1 | 3 |
| | (1 3 5)(2 4 6) | 2 | 3^2 |
| | (1 4)(2 5)(3 6) | 3 | 3^3 |
| | (1 5 3)(2 6 4) | 2 | 3^2 |
| | (1 6 5 4 3 2) | 1 | 3 |
| reflections | (1 6)(2 5)(3 4) | 3 | 3^3 |
| | (1 2)(3 6)(4 5) | 3 | 3^3 |
| | (1 4)(2 3)(5 6) | 3 | 3^3 |
| | (1)(4)(2 6)(3 5) | 4 | 3^4 |
| | (2)(5)(1 3)(4 6) | 4 | 3^4 |
| | (3)(6)(1 5)(2 4) | 4 | 3^4 |
| | | | |

By the Counting Theorem, the number of orbits is

$$\begin{aligned}
 & \frac{1}{12}(3^6 + 2 \times 3 + 2 \times 3^2 + 4 \times 3^3 + 3 \times 3^4) \\
 &= \frac{1}{12} \times 3(3^5 + 2 + 2 \times 3 + 4 \times 3^2 + 3 \times 3^3) \\
 &= \frac{1}{4}(3 \times 81 + 2 + 6 + 36 + 81) \\
 &= \frac{1}{4}(4 \times 81 + 44) \\
 &= 81 + 11 \\
 &= 92.
 \end{aligned}$$

Thus there are 92 different coloured bangles.

We can reduce the amount that we have to write down in the table in the solution to Worked Exercise E77 by recognising symmetries in $S(\square)$ that are of the same geometric type and hence will give permutations with the same cycle structure. This gives the following more concise table.

| Symmetry g | Example permutation | Number of cycles | $ \text{Fix } g $ |
|-----------------------------------|---------------------|------------------|-------------------|
| e | (1)(2)(3)(4)(5)(6) | 6 | 3^6 |
| 2 rotations, through $\pm\pi/3$ | (1 2 3 4 5 6) | 1 | 3 |
| 2 rotations, through $\pm 2\pi/3$ | (1 3 5)(2 4 6) | 2 | 3^2 |
| rotation through π | (1 4)(2 5)(3 6) | 3 | 3^3 |
| 3 reflections not through beads | (1 6)(2 5)(3 4) | 3 | 3^3 |
| 3 reflections through beads | (1)(4)(2 6)(3 5) | 4 | 3^4 |

Exercise E186

Use the Counting Theorem to determine how many different bangles decorated with *five* equally spaced beads can be made, if beads are available in just *two* colours. Hence check your answer to Exercise E174(b) in Subsection 4.1.

In the next worked exercise the chessboard problem from Subsection 4.1 is solved using the Counting Theorem. The solution does not use a table of permutations to find the sizes of the fixed sets: that would be impractical, as each permutation would contain 64 symbols! Instead, it uses the type of argument that you saw in Worked Exercise E74 in the previous subsection.

Worked Exercise E78

How many different patterns can be made by colouring the squares of a chessboard either black or white?

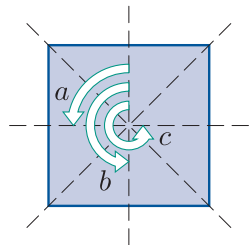


Figure 72 $S^+(\square)$

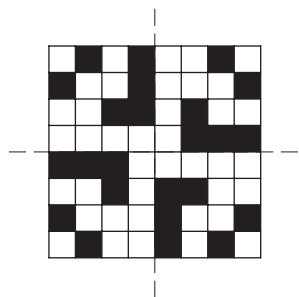


Figure 73 A coloured chessboard fixed by a

Solution

We are regarding two coloured chessboards as the same if one can be rotated to give the other. So we consider the action of the group $S^+(\square)$ (see Figure 72) on the set of all possible coloured chessboards in fixed positions.

We find the size of the fixed set of each symmetry in $S^+(\square)$ under this group action.

- First consider the identity symmetry e . It fixes all the coloured chessboards. There are 64 small squares, each coloured one of two colours, so the number of coloured chessboards is 2^{64} . Hence

$$|\text{Fix } e| = 2^{64}.$$

- Now consider the symmetry a . The coloured chessboards fixed by a are those in which each square is the same colour as the three squares onto which it is mapped under successive quarter turns (an example is shown in Figure 73). There are 2^{16} different ways to colour one quarter of such a chessboard, and this colouring determines the colours of the squares in each of the other quarters of the chessboard. Thus

$$|\text{Fix } a| = 2^{16}.$$

By a similar argument,

$$|\text{Fix } c| = 2^{16}.$$

- Finally consider the symmetry b . The coloured chessboards fixed by b are those in which each square is the same colour as the square onto which it is mapped under a half turn (an example is shown in Figure 74). There are 2^{32} different ways to colour one half of such a chessboard, and this colouring determines the colours of the squares in the other half. Thus

$$|\text{Fix } b| = 2^{32}.$$

By the Counting Theorem, the number of orbits is

$$\begin{aligned} \frac{1}{4}(2^{64} + 2 \times 2^{16} + 2^{32}) &= \frac{1}{4}(2^{64} + 2^{17} + 2^{32}) \\ &= \frac{1}{4} \times 2^{17}(2^{47} + 1 + 2^{15}) \\ &= 2^{15}(2^{47} + 2^{15} + 1). \end{aligned}$$

This is the number of different coloured chessboards.

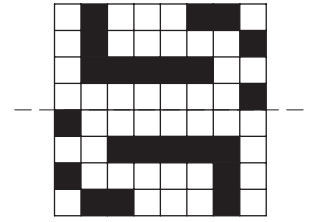


Figure 74 A coloured chessboard fixed by b

The answer found in Worked Exercise E78 is approximately 4.6×10^{18} .

Exercise E187

Use the Counting Theorem to determine how many different patterns can be made by colouring the squares of a 4×4 chessboard either black or white, when we regard two chessboards as the same if one can be obtained by rotating the other.

In the final worked exercise in this section the cube problem from Subsection 4.1 is solved using the Counting Theorem. This involves considering the action of the group $S^+(\text{cube})$ of rotations of the cube on the set of all possible coloured cubes in fixed positions. The group $S^+(\text{cube})$ has 24 elements, so it would be time-consuming to find the size of the fixed set of each of its elements individually. Instead, we collect together symmetries that are of the same geometric type and hence have fixed sets of the same size.

The solution given below includes two different versions of the part of the solution in which the sizes of the fixed sets are found. The first version uses the permutation method, and the second version does not.

Worked Exercise E79

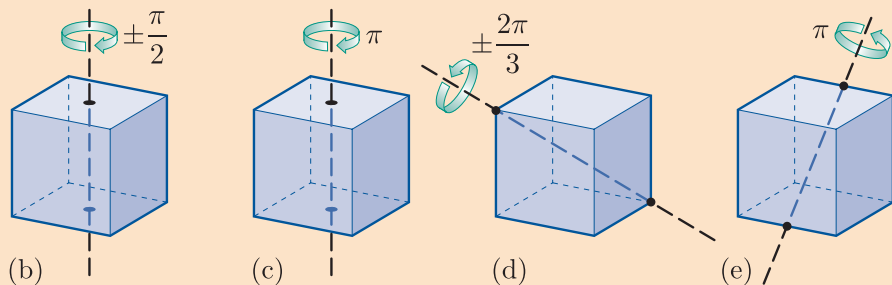
How many different coloured cubes are there with each face painted blue, yellow or red?

Solution

We are regarding two coloured cubes as the same if one can be obtained by rotating the other. So we consider the action of the group $S^+(\text{cube})$ on the set of all possible coloured cubes in fixed positions. There are 3^6 coloured cubes in fixed positions.

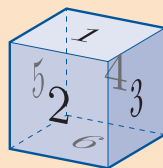
The symmetries in $S^+(\text{cube})$ are of five different geometric types, as follows. Types (b)–(e) are illustrated below.

- (a) The identity symmetry.
- (b) Rotations through $\pm\pi/2$ about axes through midpoints of opposite faces (three such axes; two such rotations about each).
- (c) Rotations through π about axes through midpoints of opposite faces (three such axes; one such rotation about each).
- (d) Rotations through $\pm 2\pi/3$ about axes through opposite vertices (four such axes; two such rotations about each).
- (e) Rotations through π about axes through midpoints of opposite edges (six such axes; one such rotation about each).



Finding the sizes of the fixed sets using the permutation method

We can label the cube as shown below.



The sizes of the fixed sets for the group action are as given below.

| Symmetry g | Example permutation | Number of cycles | $ \text{Fix } g $ |
|------------------------------|----------------------|------------------|-------------------|
| identity symmetry (type (a)) | $(1)(2)(3)(4)(5)(6)$ | 6 | 3^6 |
| 6 rotations of type (b) | $(1)(2\ 3\ 4\ 5)(6)$ | 3 | 3^3 |
| 3 rotations of type (c) | $(1)(2\ 4)(3\ 5)(6)$ | 4 | 3^4 |
| 8 rotations of type (d) | $(1\ 2\ 5)(3\ 6\ 4)$ | 2 | 3^2 |
| 6 rotations of type (e) | $(1\ 4)(2\ 6)(3\ 5)$ | 3 | 3^3 |

Alternative: finding the sizes of the fixed sets without using the permutation method

We consider the five different geometric types of symmetries in $S^+(\text{cube})$ in turn.

- (a) **The identity symmetry (type (a)).** This fixes all the coloured cubes, so $|\text{Fix } e| = 3^6$.
- (b) **Six rotations of type (b).** Let g be such a rotation. The coloured cubes fixed by g are those in which the four faces not intersected by the axis of rotation have the same colour. So for such a cube the two faces intersected by the axis can have any colours, and the other four faces must have the same colour (as illustrated in Figure 75, with Greek letters representing the colours). Thus $|\text{Fix } g| = 3^3$.
- (c) **Three rotations of type (c).** Let g be such a rotation. The coloured cubes fixed by g are those in which each of the four faces not intersected by the axis of rotation has the same colour as its opposite face. So for such a cube the two faces intersected by the axis can have any colours, but, for the other four faces, opposite faces must have the same colour (as illustrated in Figure 76). Thus $|\text{Fix } g| = 3^4$.
- (d) **Eight rotations of type (d).** Let g be such a rotation. The coloured cubes fixed by g are those in which, for each of the two vertices on the axis of rotation, the three adjacent faces have the same colour (as illustrated in Figure 77). Thus $|\text{Fix } g| = 3^2$.
- (e) **Six rotations of type (e).** Let g be such a rotation. The coloured cubes fixed by g are those in which the two faces not touching the axis of rotation have the same colour and also, for each edge intersected by the axis of rotation, the two adjacent faces have the same colour (as illustrated in Figure 78). (The rotation g transposes the six faces in three pairs.) Thus $|\text{Fix } g| = 3^3$.

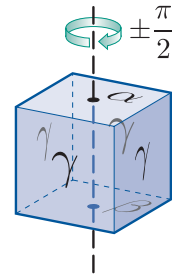


Figure 75 Colours for type (b)

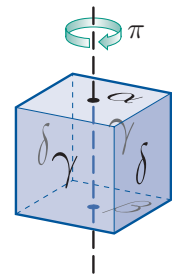


Figure 76 Colours for type (c)

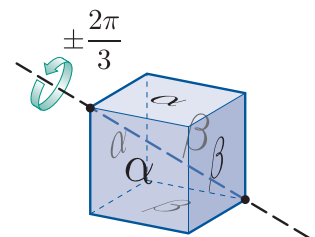


Figure 77 Colours for type (d)

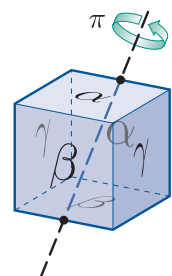


Figure 78 Colours for type (e)

Applying the Counting Theorem

By the Counting Theorem, the number of orbits is

$$\begin{aligned}
 & \frac{1}{24} (3^6 + 6 \times 3^3 + 3 \times 3^4 + 8 \times 3^2 + 6 \times 3^3) \\
 &= \frac{1}{24} \times 3^2 (3^4 + 6 \times 3 + 3 \times 3^2 + 8 + 6 \times 3) \\
 &= \frac{3}{8} (81 + 18 + 27 + 8 + 18) \\
 &= \frac{3}{8} \times 152 \\
 &= 3 \times 19 \\
 &= 57.
 \end{aligned}$$

Thus there are 57 different coloured cubes.

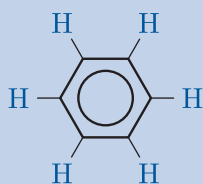
Exercise E188

How many different coloured cubes are there with each face painted blue or yellow?

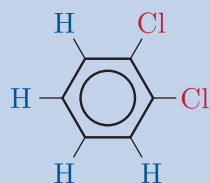
The Counting Theorem and chemical molecules

The Counting Theorem can be applied to count chemical compounds.

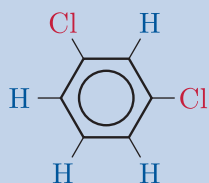
For example, *benzene* is a compound with molecular formula C_6H_6 whose molecules consist of six carbon atoms joined in a ring with a hydrogen atom attached to each, as illustrated below. (In the diagram the carbon atoms are not labelled, and the circle is a convention that indicates that the electrons forming the bonds between the carbon atoms are equally distributed.)



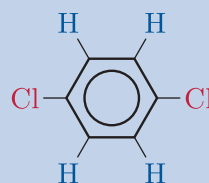
Chlorinated benzenes result when some of the hydrogen atoms in a benzene molecule are replaced by chlorine atoms. Replacing one hydrogen atom gives *chlorobenzene*, replacing two gives *dichlorobenzene*, replacing three gives *trichlorobenzene*, and so on. However, for some numbers of replaced hydrogen atoms there is more than one way to replace them. For example, the three different ways to replace two hydrogen atoms are shown below. These three molecules give *isomers* of dichlorobenzene. In general, isomers of a chemical compound are compounds that have the same molecular formula but different arrangements of the atoms in each molecule. They can have very different physical and chemical properties.



1,2-dichlorobenzene



1,3-dichlorobenzene



1,4-dichlorobenzene

Because the hydrogen and chlorine atoms in a chlorinated benzene molecule have a hexagonal arrangement, the problem of counting the number of different chlorinated benzenes is exactly the same as the problem of counting the number of six-bead bangles that you met earlier in this section, except with only two ‘colours’ (the elements hydrogen and chlorine) rather than three.

So the number of chlorinated benzenes can be worked out by changing the number of colours from three to two in the solution to Worked Exercise E77. Doing this gives the answer

$$\begin{aligned}
 & \frac{1}{12}(2^6 + 2 \times 2 + 2 \times 2^2 + 4 \times 2^3 + 3 \times 2^4) \\
 &= \frac{1}{12} \times 4(2^4 + 1 + 2 + 2^3 + 3 \times 2^2) \\
 &= \frac{1}{3}(16 + 1 + 2 + 8 + 12) \\
 &= \frac{1}{3} \times 39 \\
 &= 13.
 \end{aligned}$$

This count includes the possibility of six hydrogen atoms and no chlorine atoms, that is, benzene itself, so there are 12 different chlorinated benzenes.

Of course this count does not tell us how many isomers there are of each of dichlorobenzene, trichlorobenzene, and so on. However, there is a generalisation of the Counting Theorem known as the *Pólya Enumeration Theorem* that can be used to obtain a polynomial that provides this type of information. In the case of the chlorinated benzenes, whose underlying structure has a fairly small symmetry group, the information can be obtained quickly by drawing the different possibilities. However, for more complicated molecules there are many more possibilities and the Pólya Enumeration Theorem can provide the information much more easily.

The Pólya Enumeration Theorem was first published in 1927 by the American mathematician John Howard Redfield (1879–1944), and is sometimes known as the Redfield–Pólya Theorem. It was rediscovered independently by the Hungarian mathematician George Pólya (1887–1985). He published the result in 1937 in a paper that included the dichlorobenzene example above, as well as applications to more complicated molecules with larger symmetry groups. The paper led to an area of mathematical research known as *enumerative graph theory*.



George Pólya

Proof of the Counting Theorem

Here is a proof of the Counting Theorem.

Theorem E69 Counting Theorem

Let \wedge be an action of a finite group G on a finite set X . Then the number of orbits of \wedge is given by

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix } g|.$$

Proof Let the number of orbits of \wedge be t .

Suppose that we find the size of $\text{Stab } x$ for each element x in the set X and add up all these numbers: this gives the sum

$$\sum_{x \in X} |\text{Stab } x|.$$

We will get the same answer if we split the set X into the t orbits of \wedge , find the value of

$$\sum_{x \in B} |\text{Stab } x|$$

for each individual orbit B , and then add up these t values. Now for any orbit B of \wedge , we have

$$\begin{aligned} \sum_{x \in B} |\text{Stab } x| &= \sum_{x \in B} \frac{|G|}{|\text{Orb } x|} \quad (\text{by the Orbit-Stabiliser Theorem}) \\ &= |G| \sum_{x \in B} \frac{1}{|\text{Orb } x|} \\ &= |G| \sum_{x \in B} \frac{1}{|B|} \quad (\text{since } \text{Orb } x = B \text{ for each } x \in B) \\ &= |G| \times |B| \times \frac{1}{|B|} \\ &\quad (\text{since there are } |B| \text{ terms in the summation, each equal to } 1/|B|) \\ &= |G|. \end{aligned}$$

Adding up this value for all t orbits gives $t|G|$, so

$$\sum_{x \in X} |\text{Stab } x| = t|G|.$$

This equation can be rearranged as

$$t = \frac{1}{|G|} \sum_{x \in X} |\text{Stab } x|.$$

We can now complete the proof by showing that

$$\sum_{x \in X} |\text{Stab } x| = \sum_{g \in G} |\text{Fix } g|.$$

To do this, consider a table whose row headings are all the elements of the group G and whose column headings are all the elements of the set X . For each g in G and each x in X such that g fixes x , we enter a tick in the cell corresponding to g and x , as illustrated below.

| | | X | | | | | | | |
|-----|----------|-----|---|-----|-----|-----|-----|---|-----|
| | | ... | | x | | ... | | | |
| G | \vdots | | | | | | | | |
| | g | ... | ✓ | ✓ | ... | ✓ | ... | ✓ | ... |
| | \vdots | | | | | | | | |
| | | | | | | ✓ | | | |
| | | | | | | ✓ | | | |
| | | | | | | | | | |

For each x in X , the number of ticks in the column headed x is the number of elements of G that fix x , which is $|\text{Stab } x|$. Summing over all the columns, we see that the total number of ticks in the table is

$$\sum_{x \in X} |\text{Stab } x|.$$

But also, for each g in G , the number of ticks in the row headed g is the number of elements of X fixed by g , which is $|\text{Fix } g|$. Summing over all the rows, we see that the total number of ticks in the table is

$$\sum_{g \in G} |\text{Fix } g|.$$

Thus

$$\sum_{x \in X} |\text{Stab } x| = \sum_{g \in G} |\text{Fix } g|.$$

This completes the proof. ■

5 Group actions and groups of permutations (optional)

In this short optional section you can learn a little more about the nature of group actions, particularly those that are not *faithful*, that is, in which two or more elements of the group permute the elements of the set in the same way.

In Exercise E138 in Subsection 1.2 you considered the action of the group $S(\square)$ (see Figure 79) on the set $\{R, S, T, U\}$ of lines of symmetry of the square (shown on a single diagram in Figure 80). You saw that the elements of $S(\square)$ permute the lines of symmetry of the square as shown in the table below. Here i is the identity permutation of $\{R, S, T, U\}$.

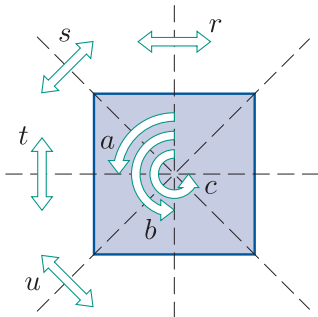


Figure 79 $S(\square)$

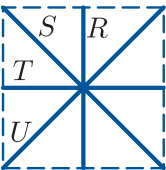


Figure 80 The lines of symmetry of the square

| Element g | Permutation |
|-------------|----------------|
| e | i |
| a | $(R\ T)(S\ U)$ |
| b | i |
| c | $(R\ T)(S\ U)$ |
| r | $(S\ U)$ |
| s | $(R\ T)$ |
| t | $(S\ U)$ |
| u | $(R\ T)$ |

Thus for this group action the group $S(\square)$ splits into four subsets, namely

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\} \quad \text{and} \quad \{s, u\},$$

such that the group elements in each subset permute the elements of the set $\{R, S, T, U\}$ in the same way.

In general, as mentioned after Exercise E138, whenever a finite group G acts on a set X , the group G can be partitioned into subsets of *equal size* such that the group elements in each subset permute the elements of X in the same way. In this subsection you will meet a theorem that explains why this is, and tells you more.

First we need a preliminary theorem, Theorem E70 below. Remember that a *permutation* of a (finite or infinite) set X is a one-to-one and onto function from X to itself. We denote the set of all permutations of a set X by $\text{Sym } X$. For example, for any natural number n we have $\text{Sym}\{1, 2, \dots, n\} = S_n$.

Theorem B52 in Unit B3 states that for any natural number n the set S_n of all permutations of the set $\{1, 2, \dots, n\}$ is a group under function composition. Theorem E70 below generalises this theorem to apply to permutations of *any* set, no matter whether it is finite or infinite. Its proof is much the same as the proof of Theorem B52.

Theorem E70

Let X be any set (finite or infinite). Then the set $\text{Sym } X$ of all permutations of the set X is a group under function composition.

Proof We check that the four group axioms hold for $(\text{Sym } X, \circ)$ (where \circ represents function composition).

G1 Closure

A composite of any two one-to-one and onto functions from X to X is a one-to-one and onto function from X to X . Thus $\text{Sym } X$ is closed under function composition.

G2 Associativity

Function composition is associative.

G3 Identity

The identity function, say i , on X is an identity element for function composition in $\text{Sym } X$.

G4 Inverses

Every one-to-one and onto function f from X to X has an inverse function f^{-1} that maps from X to X and satisfies $f \circ f^{-1} = i = f^{-1} \circ f$. That is, each element f of $\text{Sym } X$ has an inverse f^{-1} in $\text{Sym } X$ with respect to function composition.

Hence $(\text{Sym } X, \circ)$ is a group. ■

For any set X , the group $\text{Sym } X$ of all permutations of X is called the **symmetric group** on X . The identity element of this group, which is the identity function on X , is called the **identity permutation** of X .

We can now prove the following illuminating theorem. In the statement of this theorem the symbol $*$ is used instead of our usual symbol \circ to denote the binary operation of a general group G , because the symbol \circ is needed to represent function composition.

Theorem E71

Let \wedge be an action of a group $(G, *)$ on a set X . For each g in G , let f_g be the permutation in $\text{Sym } X$ given by

$$f_g(x) = g \wedge x$$

for all $x \in X$. (That is, for each g in G the permutation f_g is the permutation of X that is the effect of g under \wedge .) Then the mapping

$$\begin{aligned}\phi : (G, *) &\longrightarrow (\text{Sym } X, \circ) \\ g &\longmapsto f_g\end{aligned}$$

is a homomorphism.

Proof Let $g, h \in G$. We have to show that

$$\phi(g * h) = \phi(g) \circ \phi(h);$$

that is,

$$f_{g*h} = f_g \circ f_h.$$

Now f_{g*h} , f_g and f_h are all functions with domain X , so to show that the equation above holds we have to show that

$$f_{g*h}(x) = (f_g \circ f_h)(x)$$

for all $x \in X$. To do this, let $x \in X$. Then

$$\begin{aligned}f_{g*h}(x) &= (g * h) \wedge x \quad (\text{by the definition of } f_{g*h}) \\ &= g \wedge (h \wedge x) \quad (\text{by axiom GA3}) \\ &= f_g(f_h(x)) \quad (\text{by the definition of } f_h \text{ and } f_g) \\ &= (f_g \circ f_h)(x) \quad (\text{by the definition of function composition}).\end{aligned}$$

Thus ϕ is a homomorphism. ■

To illustrate Theorem E71, consider once again the action of the group $S(\square)$ on the set $\{R, S, T, U\}$ of lines of symmetry of the square. As mentioned earlier in this subsection, the elements of $S(\square)$ permute the elements of $\{R, S, T, U\}$ as follows, where i is the identity permutation of X .

| Element g | Permutation |
|-------------|----------------|
| e | i |
| a | $(R\ T)(S\ U)$ |
| b | i |
| c | $(R\ T)(S\ U)$ |
| r | $(S\ U)$ |
| s | $(R\ T)$ |
| t | $(S\ U)$ |
| u | $(R\ T)$ |

Theorem E71 tells us that the following mapping ϕ is a homomorphism.

$$\begin{aligned}\phi : (S(\square), \circ) &\longrightarrow (\text{Sym}\{R, S, T, U\}, \circ) \\ e &\longmapsto i \\ a &\longmapsto (R\ T)(S\ U) \\ b &\longmapsto i \\ c &\longmapsto (R\ T)(S\ U) \\ r &\longmapsto (S\ U) \\ s &\longmapsto (R\ T) \\ t &\longmapsto (S\ U) \\ u &\longmapsto (R\ T)\end{aligned}$$

Exercise E189

In each of parts (a) and (b) below, write down the homomorphism $\phi : (S(\square), \circ) \longrightarrow (\text{Sym}\{X\}, \circ)$ as defined in Theorem E71 for the action of the group $S(\square)$ on the set X whose elements are the modified hexagons shown.

Use the labels for the elements of $S(\square)$ shown in Figure 81.

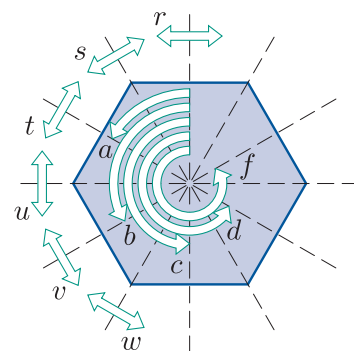
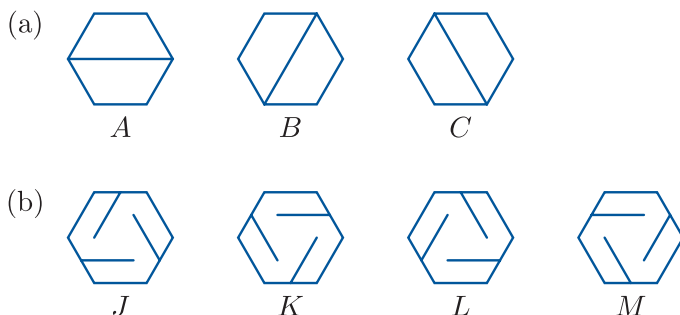


Figure 81 $S(\square)$

We can obtain several useful results about group actions by applying the results about homomorphisms that you met in Unit E3 to the homomorphisms obtained from group actions as defined in Theorem E71. These include the following results.

Corollary E72

Let \wedge be an action of a group $(G, *)$ on a set X . Then the following hold for \wedge .

- (a) The set of permutations of X given by the elements of G under \wedge is a group under function composition.
- (b) The set E of elements of G that behave as the identity permutation of X is a normal subgroup of G .
- (c) Two elements of G behave as the same permutation of X if and only if they lie in the same coset of E .

Proof Let $\phi : (G, *) \longrightarrow (\text{Sym } X, \circ)$ be the homomorphism obtained from \wedge as defined in Theorem E71.

- (a) The set of permutations of X given by the elements of G under \wedge is the image of ϕ . Since the image of any homomorphism is a subgroup of the codomain group (by Theorem E47 in Unit E3), this set is a group under function composition.
- (b) The set E of elements of G that behave as the identity permutation of X under \wedge is the kernel of ϕ . Since the kernel of any homomorphism is a normal subgroup of the domain group (by Theorem E51 in Unit E3), E is a normal subgroup of G .
- (c) By Theorem E54 in Unit E3, two elements of G have the same image under ϕ if and only if they lie in the same coset of $\text{Ker } \phi$ in G . That is, two elements of G behave as the same permutation of X if and only if they lie in the same coset of E . ■

By Corollary E72(b) and (c), whenever a group G acts on a set X , the group G has a normal subgroup E such that all the group elements in each coset of E behave as the same permutation of X . If G is finite, then each of these cosets contains the same number of elements, because this is always the case for cosets in a finite group. This justifies the fact mentioned near the start of this section: if a finite group G acts on a set X , then the group G can be partitioned into subsets of equal size such that the group elements in each subset permute the elements of X in the same way. (If the action of G on X is faithful, then each of the subsets contains a single element.)

Exercise E190

For each of the two group actions in Exercise E189, use your solution to Exercise E189 to partition the group $S(\square)$ into subsets such that all the group elements in each subset behave as the same permutation of the set X . Write down the permutation of X corresponding to each subset.

The main theorem earlier in this section, Theorem E71, tells us that every action of a group $(G, *)$ on a set X defines a homomorphism $\phi : (G, *) \rightarrow (\text{Sym } X, \circ)$. The theorem below tells us that the converse of this theorem is also true: if $(G, *)$ is a group and X is a set then every homomorphism $\phi : (G, *) \rightarrow (\text{Sym } X, \circ)$ defines an action of $(G, *)$ on X . You may find the expression $(\phi(g))(x)$ in the statement of this theorem rather complicated. Keep in mind that the codomain of the homomorphism ϕ is $(\text{Sym } X, \circ)$, so $\phi(g)$ is a permutation of the set X and hence $(\phi(g))(x)$ is the image of x under the permutation $\phi(g)$.

Theorem E73

Let $(G, *)$ be a group, let X be a set and let $\phi : (G, *) \rightarrow (\text{Sym } X, \circ)$ be a homomorphism. Let \wedge be defined by

$$g \wedge x = (\phi(g))(x)$$

for all $g \in G$ and all $x \in X$. Then \wedge is an action of $(G, *)$ on X .

The next exercise asks you to prove Theorem E73. It involves working with expressions like the one mentioned above, so you may find it quite complicated.

Exercise E191

Prove Theorem E73.

Theorems E71 and E73 together show that if $(G, *)$ is a group and X is a set, then actions of $(G, *)$ on X and homomorphisms from $(G, *)$ to $(\text{Sym } X, \circ)$ are essentially the same objects.

Summary

In this unit you have learned what is meant by a group action on a set, and met many examples. You have studied some general properties of group actions, and seen how some of the concepts and results that you met in earlier group theory units, such as conjugacy, Lagrange's Theorem and homomorphisms, can be viewed as particular cases of concepts and results relating to group actions. Finally, you met the *Counting Theorem* and saw how it can be used to solve counting problems that involve symmetry.

Now that you have reached the end of the group theory part of M208, you should be able to recognise how group theory reveals links and similarities in a variety of different concepts, and hence increases our understanding of them. You may be starting to appreciate the beauty and elegance of group theory as a mathematical theory in its own right, and beginning to see how it can provide powerful tools for solving some types of problems. You saw an example of its use when you solved counting problems using the Counting Theorem, but it is also used in other areas, such as cryptography, coding theory and the design of experiments. Group theory is part of the mathematical subject area known as *abstract algebra*, which is concerned with mathematical structures such as groups, fields and vector spaces.

Learning outcomes

After working through this unit, you should be able to:

- explain what is meant by a *group action*
- check the group action axioms
- explain what is meant by the *orbit* $\text{Orb } x$ and the *stabiliser* $\text{Stab } x$ of an element x of a set under the action of a group
- understand that the orbits of a group action form a partition of the set on which the group acts
- understand that the stabiliser of a set element under a group action is a subgroup of the group that is acting
- determine orbits and stabilisers for a group action
- understand the *Orbit–Stabiliser Theorem*
- understand various ways in which a group can act on itself or on other groups
- explain what is meant by the *fixed set* $\text{Fix } g$ of an element g of a group that acts on a set
- determine fixed sets for a group action
- understand the *Counting Theorem*
- use the Counting Theorem to solve counting problems involving symmetry.

Solutions to exercises

Solution to Exercise E134

- (a) (i) $r \wedge 2 = 3$
 (ii) $b \wedge 1 = 3$
 (b) (i) $b \wedge B = D$
 (ii) $s \wedge B = B$
 (c) (i) $(1\ 3\ 2) \wedge 2 = 1$
 (ii) $(1\ 2) \wedge 3 = 3$
 (d) (i) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \wedge \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 7 \\ 2 \end{pmatrix}$
 (ii) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \wedge \begin{pmatrix} -1 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -1 \\ 4 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$
 (e) (i) $3 \wedge 7.4 = 3 + 7.4 = 10.4$
 (ii) $1 \wedge -0.3 = 1 + (-0.3) = 0.7$

Solution to Exercise E135

We check the group action axioms.

GA1 Let $g \in G$ and let $x \in X$. Since g fixes or transposes the symbols 4 and 5, it maps each of the symbols 1, 2 and 3 to 1, 2 or 3. Therefore

$$g \wedge x = g(x) \in X.$$

Thus axiom GA1 holds.

GA2 The identity element e of G is the identity permutation of $\{1, 2, 3, 4, 5\}$. So for each x in $X = \{1, 2, 3\}$, we have

$$e \wedge x = e(x) = x.$$

Thus axiom GA2 holds.

GA3 Let $g, h \in G$ and let $x \in X$. Then

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge (h(x)) \quad (\text{by the definition of } \wedge) \\ &= g(h(x)) \quad (\text{by the definition of } \wedge) \\ &= (g \circ h)(x) \\ &\quad (\text{by the definition of function composition}) \\ &= (g \circ h) \wedge x \quad (\text{by the definition of } \wedge). \end{aligned}$$

Thus axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

Solution to Exercise E136

(a) This mapping effect \wedge does not satisfy axiom GA1 (closure). For example, $(1\ 4) \in S_5$ and $1 \in \{1, 2, 3\}$, but

$$(1\ 4) \wedge 1 = 4 \notin \{1, 2, 3\}.$$

Hence \wedge is not a group action.

(This mapping effect \wedge does satisfy axioms GA2 and GA3.)

(b) This mapping effect \wedge does not satisfy axiom GA2 (identity).

To see this, note that the identity element of the group (\mathbb{R}^*, \times) is 1, and, for example, $(4, 4) \in \mathbb{R}^2$, but

$$1 \wedge (4, 4) = (4 + 1, 4 + 1) = (5, 5) \neq (4, 4).$$

Hence \wedge is not a group action.

(This mapping effect \wedge does satisfy axiom GA1. However, it does not satisfy axiom GA3. To satisfy this axiom it would have to satisfy

$$g \wedge (h \wedge (x, y)) = (g \times h) \wedge (x, y)$$

for all $g, h \in \mathbb{R}^*$ and all $(x, y) \in \mathbb{R}^2$. However, for example, $1, 2 \in \mathbb{R}^*$ and $(1, 1) \in \mathbb{R}^2$, but

$$1 \wedge (2 \wedge (1, 1)) = 1 \wedge (3, 3) = (4, 4)$$

whereas

$$(1 \times 2) \wedge (1, 1) = 2 \wedge (1, 1) = (3, 3).$$

Solution to Exercise E137

(a) This is a group action.

(b) The element a of $S(\square)$ maps



The first figure here is an element of X , but the second figure is not. Thus axiom GA1 does not hold. Hence \wedge is not a group action.

(c) This is a group action.

(d) This is a group action.

(e) The element a of $S^+(\square)$ maps



The first figure here is an element of X , but the second figure is not. Thus axiom GA1 does not hold. Hence \wedge is not a group action.

(f) This is a group action.

(g) This is a group action.

(h) This is a group action. (Each symmetry of the square maps any plane figure A in X to another plane figure, which also lies in X since X contains all plane figures.)

(i) This is a group action.

(j) By rotating the tetrahedron we can map one of the three edges in X to an edge that does not lie in X . For example, we can map



Thus axiom GA1 does not hold. Hence \wedge is not a group action.

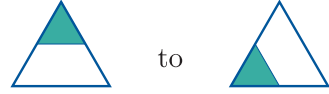
Solution to Exercise E138

The permutations are as follows. Here the identity permutation of $\{R, S, T, U\}$ is denoted by i , since e is used to denote the identity element of $S(\square)$.

| Element g | Permutation |
|-------------|----------------|
| e | i |
| a | $(R\ T)(S\ U)$ |
| b | i |
| c | $(R\ T)(S\ U)$ |
| r | $(S\ U)$ |
| s | $(R\ T)$ |
| t | $(S\ U)$ |
| u | $(R\ T)$ |

Solution to Exercise E139

(a) The element a of $S(\triangle)$ maps



The first coloured figure here is an element of X , but the second is not. Thus axiom GA1 does not hold. Hence \wedge is not a group action.

(b) This is a group action.

(c) This is a group action. (The set X includes every possible colour combination, so the result of applying any symmetry of the square to an element of X must be another element of X .)

Solution to Exercise E140

We check the group action axioms.

GA1 Let $g \in \mathbb{Z}$ and let $x \in \mathbb{R}$. Then

$$g \wedge x = x - g \in \mathbb{R}.$$

Thus axiom GA1 holds.

GA2 The identity element of the group $(\mathbb{Z}, +)$ is 0.

Let $x \in \mathbb{R}$. Then

$$0 \wedge x = x - 0 = x.$$

Thus axiom GA2 holds.

GA3 Let $g, h \in \mathbb{Z}$ and let $x \in \mathbb{R}$. We have to show that

$$g \wedge (h \wedge x) = (g + h) \wedge x.$$

Now

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge (x - h) \quad (\text{by the definition of } \wedge) \\ &= (x - h) - g \quad (\text{by the definition of } \wedge) \\ &= x - (h + g) \\ &= (g + h) \wedge x \quad (\text{by the definition of } \wedge). \end{aligned}$$

Thus axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

Solution to Exercise E141

This mapping effect \wedge does not satisfy axiom GA2.

To see this, note that the identity element of the group $(\mathbb{Z}, +)$ is 0, and, for example, $1 \in \mathbb{R}$, but

$$0 \wedge 1 = 0 - 1 = -1 \neq 1.$$

Thus axiom GA2 does not hold.

Hence \wedge is not a group action.

(This mapping effect \wedge does not satisfy axiom GA3 either, but it does satisfy axiom GA1.)

Solution to Exercise E142

We show that the group action axioms hold.

GA1 Let $g \in \mathbb{R}$ and let $(x, y) \in \mathbb{R}^2$. Then

$$g \wedge (x, y) = (x, y + g) \in \mathbb{R}^2.$$

Thus axiom GA1 holds.

GA2 The identity element of the group $(\mathbb{R}, +)$ is 0.

Let $(x, y) \in \mathbb{R}^2$. Then

$$0 \wedge (x, y) = (x, y + 0) = (x, y).$$

Thus axiom GA2 holds.

GA3 Let $g, h \in \mathbb{R}$ and let $(x, y) \in \mathbb{R}^2$. We have to show that

$$g \wedge (h \wedge (x, y)) = (g + h) \wedge (x, y).$$

Now

$$\begin{aligned} g \wedge (h \wedge (x, y)) &= g \wedge (x, y + h) \\ &= (x, y + h + g) \\ &= (x, y + g + h) \end{aligned}$$

and

$$(g + h) \wedge (x, y) = (x, y + g + h).$$

The two expressions obtained are the same, so axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

Solution to Exercise E143

(a) We check the group action axioms.

GA1 The element (ax, y) is an element of \mathbb{R}^2 for all real numbers a, x and y , so axiom GA1 holds.

GA2 The identity element of G is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $(x, y) \in \mathbb{R}^2$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (1x, y) = (x, y).$$

So axiom GA2 holds.

GA3 Let $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in G$ and let $(x, y) \in \mathbb{R}^2$. We have to show that

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge \left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \wedge (x, y) \right) \\ = \left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right) \wedge (x, y). \end{aligned}$$

Now

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge \left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \wedge (x, y) \right) \\ = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (cx, y) \\ = (acx, y) \end{aligned}$$

and

$$\begin{aligned} \left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right) \wedge (x, y) \\ = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix} \wedge (x, y) \\ = (acx, y). \end{aligned}$$

The two expressions obtained are the same, so axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

(b) Axiom GA2 does not hold for \wedge because, for example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \wedge (2, 2) = (1 \times 2, 0 \times 2) = (2, 0) \neq (2, 2).$$

Thus \wedge is not a group action.

(Axiom GA3 does not hold either, but axiom GA1 does hold.)

(c) Axiom GA3 does not hold for \wedge .

For axiom GA3 to hold, we require that, for all

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in G \text{ and all } (x, y) \in \mathbb{R}^2,$$

$$\begin{aligned} & \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge \left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \wedge (x, y) \right) \\ &= \left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right) \wedge (x, y). \end{aligned}$$

The left-hand side of this equation is equal to

$$\begin{aligned} & \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (cx, dy + y) \\ &= (acx, b(dy + y) + dy + y) \\ &= (acx, bdy + by + dy + y) \end{aligned}$$

and the right-hand side is equal to

$$\begin{aligned} & \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix} \wedge (x, y) \\ &= (acx, (ad + b)y + y) \\ &= (acx, ady + by + y). \end{aligned}$$

The two expressions obtained are equal only if

$$bdy + by + dy + y = ady + by + y;$$

that is, only if

$$bdy + dy = ady,$$

which we can write as

$$(b - a + 1)dy = 0.$$

This equation is not true in general. For instance, if we take $a = b = d = y = 1$, it gives $1 = 0$.

So, for example, the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$ and the point $(0, 1) \in \mathbb{R}^2$ provide a counterexample to show that axiom GA3 does not hold here.

Thus \wedge is not a group action.

(Axioms GA1 and GA2 do hold.)

(It is not necessary to give the general algebraic argument above: it is sufficient just to demonstrate that there is a counterexample to axiom GA3.

However, the general argument may help us find a counterexample.)

Solution to Exercise E144

The orbits are

$$\text{Orb } 1 = \{1, 2, 3, 4\},$$

$$\text{Orb } 2 = \{1, 2, 3, 4\},$$

$$\text{Orb } 3 = \{1, 2, 3, 4\},$$

$$\text{Orb } 4 = \{1, 2, 3, 4\}.$$

(So for this group action the orbit of each element is just the whole set X on which the group acts.)

Solution to Exercise E145

The orbits are

$$\text{Orb } A = \{A\},$$

$$\text{Orb } B = \{B, C, D\},$$

$$\text{Orb } C = \{B, C, D\},$$

$$\text{Orb } D = \{B, C, D\}.$$

Solution to Exercise E146

The orbits are

$$\text{Orb } A = \{A, B\},$$

$$\text{Orb } B = \{A, B\},$$

$$\text{Orb } C = \{C, D\},$$

$$\text{Orb } D = \{C, D\}.$$

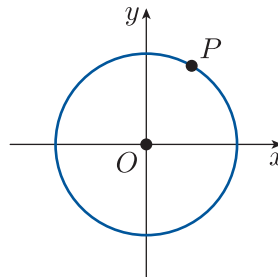
Solution to Exercise E147

The elements of the group $S(\odot)$ are the rotations about O and the reflections in the lines through O .

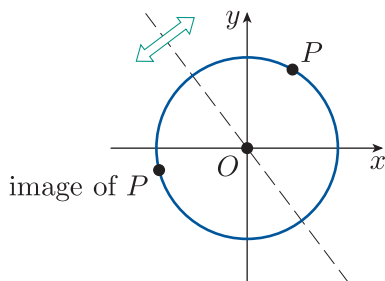
Any rotation about O and any reflection in a line through O maps O to itself, so

$$\text{Orb } O = \{O\}.$$

Now let P be any other point in \mathbb{R}^2 . The rotations in $S(\odot)$ rotate P about O , through all possible angles. So $\text{Orb } P$ certainly includes all points on the circle with centre O whose radius is the distance between O and P , as shown below.



Also, any reflection in a line through O maps P to a point on this circle, as illustrated below.



Hence $\text{Orb } P$ is this circle.

(So the orbits of the points in \mathbb{R}^2 under the action of $S(\bigcirc)$ are the same as their orbits under the action of $S^+(\bigcirc)$, which were found in Worked Exercise E63.)

Solution to Exercise E148

The orbits are

$$\{A_1, A_3, A_7, A_9\}, \quad \{A_2, A_4, A_6, A_8\}, \quad \{A_5\}.$$

(We can find them by using Strategy E7.)

Solution to Exercise E149

(a) The orbits are

$$\{A_1, A_2, A_3, A_4\}, \quad \{A_5, A_6, A_7, A_8\}.$$

(b) There is just one orbit:

$$\{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8\} = X.$$

Solution to Exercise E150

(a) There is just one orbit:

$$\{1, 2, 3, 4\}.$$

(b) The orbits are

$$\{1, 3\}, \quad \{2, 4\}.$$

(c) The orbits are

$$\{1, 4\}, \quad \{2, 3\}.$$

(d) The orbits are

$$\{1\}, \quad \{2\}, \quad \{3\}, \quad \{4\}.$$

Solution to Exercise E151

In the solution to Worked Exercise E64 it was found that for any point $(x, y) \in \mathbb{R}^2$,

$$\text{Orb}(x, y) = \{(ax, by) : a, b \in \mathbb{R}^+\}.$$

(a) Putting $(x, y) = (1, 0)$ gives

$$\begin{aligned} \text{Orb}(1, 0) &= \{(a \times 1, b \times 0) : a, b \in \mathbb{R}^+\} \\ &= \{(a, 0) : a \in \mathbb{R}^+\}. \end{aligned}$$

So $\text{Orb}(1, 0)$ is the positive part of the x -axis.

(b) Putting $(x, y) = (0, -1)$ gives

$$\begin{aligned} \text{Orb}(0, -1) &= \{(a \times 0, b \times (-1)) : a, b \in \mathbb{R}^+\} \\ &= \{(0, -b) : b \in \mathbb{R}^+\}. \end{aligned}$$

So $\text{Orb}(0, -1)$ is the negative part of the y -axis.

(c) Putting $(x, y) = (1, 1)$ gives

$$\begin{aligned} \text{Orb}(1, 1) &= \{(a \times 1, b \times 1) : a, b \in \mathbb{R}^+\} \\ &= \{(a, b) : a, b \in \mathbb{R}^+\}. \end{aligned}$$

So $\text{Orb}(1, 1)$ is the first quadrant of the plane.

(It does not include any points on the x -axis or y -axis.)

Solution to Exercise E152

The point $(0, 1)$ has still not been assigned to an orbit. We have

$$\begin{aligned} \text{Orb}(0, 1) &= \{(a \times 0, b \times 1) : a, b \in \mathbb{R}^+\} \\ &= \{(0, b) : b \in \mathbb{R}^+\}. \end{aligned}$$

So $\text{Orb}(0, 1)$ is the positive part of the y -axis.

The point $(-1, 1)$ has still not been assigned to an orbit. We have

$$\begin{aligned} \text{Orb}(-1, 1) &= \{(a \times (-1), b \times 1) : a, b \in \mathbb{R}^+\} \\ &= \{(-a, b) : a, b \in \mathbb{R}^+\}. \end{aligned}$$

So $\text{Orb}(-1, 1)$ is the second quadrant of the plane.

(It does not include any points on the x -axis or y -axis.)

The point $(-1, -1)$ has still not been assigned to an orbit. We have

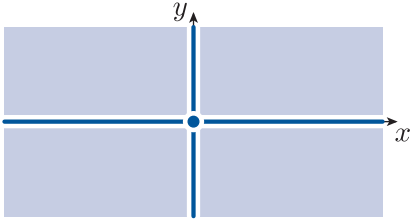
$$\begin{aligned} \text{Orb}(-1, -1) &= \{(a \times (-1), b \times (-1)) : a, b \in \mathbb{R}^+\} \\ &= \{(-a, -b) : a, b \in \mathbb{R}^+\}. \end{aligned}$$

So $\text{Orb}(-1, -1)$ is the third quadrant of the plane.

(It does not include any points on the x -axis or y -axis.)

All the points in the plane have now been assigned to orbits.

The nine orbits of the group action are sketched below.



Solution to Exercise E153

For any point $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned}\text{Orb}(x, y) &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) : \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G \right\} \\ &= \{(ax, y) : a, b \in \mathbb{R}, a \neq 0\} \\ &= \{(ax, y) : a \in \mathbb{R}^*\}.\end{aligned}$$

For any point of the form $(0, y)$ (that is, any point on the y -axis) we have

$$\text{Orb}(0, y) = \{(a \times 0, y) : a \in \mathbb{R}^*\} = \{(0, y)\}.$$

So each point on the y -axis lies in an orbit containing itself alone. For example, $\text{Orb}(0, 2) = \{(0, 2)\}$.

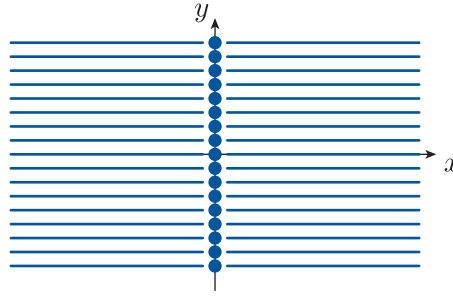
For any point of the form (x, y) where $x \neq 0$ (that is, any point not on the y -axis) we have

$$\text{Orb}(x, y) = \{(ax, y) : a \in \mathbb{R}^*\}.$$

This is the set of all points on the horizontal line through the point (x, y) , except for the point $(0, y)$. For example, $\text{Orb}(1, 2)$ is the line $y = 2$ excluding the point $(0, 2)$.

We have now found all the orbits. They are the individual points on the y -axis and the horizontal lines excluding the point on the y -axis in each such line.

They are sketched below. Each orbit that is a line continues on the other side of the y -axis.



Solution to Exercise E154

For any point $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned}\text{Orb}(x, y) &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge (x, y) : \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G \right\} \\ &= \{(ax, ay) : a, b \in \mathbb{R}, a \neq 0\} \\ &= \{(ax, ay) : a \in \mathbb{R}^*\}.\end{aligned}$$

So, for example,

$$\text{Orb}(0, 0) = \{(a \times 0, a \times 0) : a \in \mathbb{R}^*\} = \{(0, 0)\}.$$

So the orbit of the point $(0, 0)$ consists of the point $(0, 0)$ alone.

Also, for example,

$$\begin{aligned}\text{Orb}(1, 0) &= \{(a \times 1, a \times 0) : a \in \mathbb{R}^*\} \\ &= \{(a, 0) : a \in \mathbb{R}^*\},\end{aligned}$$

$$\begin{aligned}\text{Orb}(0, 1) &= \{(a \times 0, a \times 1) : a \in \mathbb{R}^*\} \\ &= \{(0, a) : a \in \mathbb{R}^*\},\end{aligned}$$

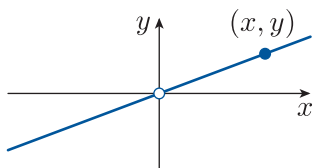
$$\begin{aligned}\text{Orb}(1, 2) &= \{(a \times 1, a \times 2) : a \in \mathbb{R}^*\} \\ &= \{(a, 2a) : a \in \mathbb{R}^*\}.\end{aligned}$$

So $\text{Orb}(1, 0)$ consists of all the points on the x -axis excluding the origin, $\text{Orb}(0, 1)$ consists of all the points on the y -axis excluding the origin, and $\text{Orb}(1, 2)$ consists of all the points on the line $y = 2x$ excluding the origin.

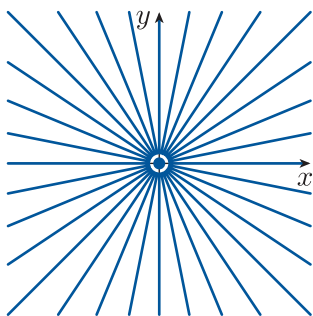
In general, as we found above, we have

$$\text{Orb}(x, y) = \{(ax, ay) : a \in \mathbb{R}^*\}.$$

If x and y are not both zero, then this set consists of all the points on the line through the origin and the point (x, y) , excluding the origin itself, as sketched below.



We have now found all the orbits. They are the origin, together with all the lines that pass through the origin, each excluding the origin. They are sketched below. (Each orbit that is a line continues on the other side of the origin.)



Solution to Exercise E155

The stabilisers are

$$\text{Stab } 1 = \{e, s\},$$

$$\text{Stab } 2 = \{e, u\},$$

$$\text{Stab } 3 = \{e, s\},$$

$$\text{Stab } 4 = \{e, u\}.$$

Solution to Exercise E156

The stabilisers are

$$\text{Stab } A = \{e, a, b, r, s, t\} = S(\triangle),$$

$$\text{Stab } B = \{e, r\},$$

$$\text{Stab } C = \{e, s\},$$

$$\text{Stab } D = \{e, t\}.$$

Solution to Exercise E157

The stabilisers are

$$\text{Stab } A = \{e, s\},$$

$$\text{Stab } B = \{e, s\},$$

$$\text{Stab } C = \{e, r\},$$

$$\text{Stab } D = \{e, r\}.$$

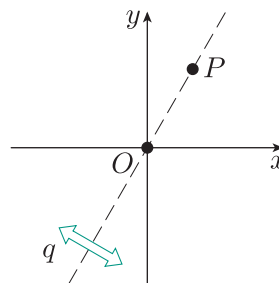
Solution to Exercise E158

The elements of the group $S(\bigcirc)$ are the rotations about O and the reflections in the lines through O .

Any rotation about O and any reflection in a line through O fixes O , so

$$\text{Stab } O = S(\bigcirc).$$

Now let P be any other point in \mathbb{R}^2 . The only rotation in $S(\bigcirc)$ that fixes P is the identity symmetry e . The only reflection in $S(\bigcirc)$ that fixes P is the reflection, say q , in the line through O and P , as illustrated below.



So

$$\text{Stab } P = \{e, q\},$$

where q is the reflection in the line through O and P .

Solution to Exercise E159

The stabilisers are

$$\text{Stab } A_1 = \{e, s\},$$

$$\text{Stab } A_2 = \{e, r\},$$

$$\text{Stab } A_3 = \{e, u\},$$

$$\text{Stab } A_4 = \{e, t\},$$

$$\text{Stab } A_5 = \{e, a, b, c, r, s, t, u\} = S(\square),$$

$$\text{Stab } A_6 = \{e, t\},$$

$$\text{Stab } A_7 = \{e, u\},$$

$$\text{Stab } A_8 = \{e, r\},$$

$$\text{Stab } A_9 = \{e, s\}.$$

The stabiliser $\text{Stab } A_5$ is a subgroup of $S(\square)$ because it is the whole group $S(\square)$. The stabiliser of each of the other modified squares consists of the identity element e of $S(\square)$ together with an element of $S(\square)$ of order 2, so it is the subgroup of $S(\square)$ generated by that element of order 2. Thus all the stabilisers are subgroups of $S(\square)$.

Solution to Exercise E160

(a) The stabiliser of each of the modified squares is $\{e\}$, which is the trivial subgroup of $S^+(\square)$.

(b) Again, the stabiliser of each of the modified squares is the trivial subgroup $\{e\}$.

Solution to Exercise E161

From the solution to Worked Exercise E69, for any point (x, y) in \mathbb{R}^2 ,

$$\text{Stab}(x, y) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : ax = x \text{ and } by = y \right\}.$$

(a) Putting $(x, y) = (2, 0)$ gives

$$\begin{aligned} \text{Stab}(2, 0) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a \times 2 = 2 \text{ and } b \times 0 = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : 2a = 2 \text{ and } 0 = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a = 1 \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} : b \in \mathbb{R}^+ \right\}. \end{aligned}$$

(This is the same subgroup of (G, \times) as $\text{Stab}(-1, 0)$, found in Worked Exercise E69(b).)

(b) Putting $(x, y) = (0, 5)$ gives

$$\begin{aligned} \text{Stab}(0, 5) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a \times 0 = 0 \text{ and } b \times 5 = 5 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : 0 = 0 \text{ and } 5b = 5 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : b = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^+ \right\}. \end{aligned}$$

Solution to Exercise E162

From the solution to Worked Exercise E69, for any point $(x, y) \in \mathbb{R}^2$,

$$\text{Stab}(x, y) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : ax = x \text{ and } by = y \right\}.$$

(a) Consider a point of the form $(x, 0)$ where $x \in \mathbb{R}^*$. By the expression for $\text{Stab}(x, y)$ above, we have

$$\begin{aligned} \text{Stab}(x, 0) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : ax = x \text{ and } b \times 0 = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : ax = x \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a = 1 \right\} \quad (\text{since } x \neq 0) \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} : b \in \mathbb{R}^+ \right\}. \end{aligned}$$

This is the same subgroup as found in Exercise E161(a).

(b) Consider a point of the form $(0, y)$ where $y \in \mathbb{R}^*$. By the expression for $\text{Stab}(x, y)$ above, we have

$$\begin{aligned} \text{Stab}(0, y) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a \times 0 = 0 \text{ and } by = y \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : by = y \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : b = 1 \right\} \quad (\text{since } y \neq 0) \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^+ \right\}. \end{aligned}$$

This is the same subgroup as found in Exercise E161(b).

(c) Consider a point of the form (x, y) where $x, y \in \mathbb{R}^*$. By the expression for $\text{Stab}(x, y)$ above, we have

$$\begin{aligned} \text{Stab}(x, y) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : ax = x \text{ and } by = y \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G : a = 1 \text{ and } b = 1 \right\} \\ &\quad (\text{since } x, y \neq 0) \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}. \end{aligned}$$

This is the trivial subgroup of (G, \times) .

Solution to Exercise E163

For any point $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned}
 \text{Stab}(x, y) &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G : \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (x, y) \right\} \\
 &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G : (ax, y) = (x, y) \right\} \\
 &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G : ax = x \text{ and } y = y \right\} \\
 &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G : ax = x \right\}.
 \end{aligned}$$

Since we can simplify the equation $ax = x$ in the expression above if we know that $x \neq 0$, we now consider the cases $x \neq 0$ and $x = 0$ separately.

For any point $(x, y) \in \mathbb{R}^2$ with $x \neq 0$ (that is, any point not on the y -axis), we have

$$\begin{aligned}
 \text{Stab}(x, y) &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G : ax = x \right\} \\
 &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G : a = 1 \right\} \\
 &\quad \text{(since } x \neq 0) \\
 &= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}.
 \end{aligned}$$

For any point $(0, y) \in \mathbb{R}^2$ (that is, any point on the y -axis), we have

$$\begin{aligned}
 \text{Stab}(0, y) &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G : a \times 0 = 0 \right\} \\
 &= G.
 \end{aligned}$$

In summary, the stabiliser of any point on the y -axis is the whole group G , and the stabiliser of any other point is the subgroup

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

Solution to Exercise E164

For any point $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned}
 \text{Stab}(x, y) &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G : \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \wedge (x, y) = (x, y) \right\} \\
 &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G : (ax, ay) = (x, y) \right\} \\
 &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G : ax = x \text{ and } ay = y \right\}.
 \end{aligned}$$

Now if we know that $x \neq 0$ then we can simplify the equation $ax = x$ to $a = 1$. Similarly, if we know that $y \neq 0$ then we can simplify the equation $ay = y$ to $a = 1$. So we now split into two cases: the case where *either* $x \neq 0$ *or* $y \neq 0$ (or both), that is, the case where x and y are not both zero, and the remaining case, which is $x = y = 0$.

For any point $(x, y) \in \mathbb{R}^2$ such that $x \neq 0$ or $y \neq 0$ (that is, any point except the origin), we have

$$\begin{aligned}
 \text{Stab}(x, y) &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G : a = 1 \right\} \\
 &= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}.
 \end{aligned}$$

The only remaining point is the origin, for which we have

$$\begin{aligned}
 \text{Stab}(0, 0) &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G : a \times 0 = 0 \text{ and } a \times 0 = 0 \right\} \\
 &= G.
 \end{aligned}$$

In summary, the stabiliser of the origin is the whole group G , and the stabiliser of any other point is the subgroup

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

Solution to Exercise E165

| A | $\text{Orb } A$ | $\text{Stab } A$ | $ \text{Orb } A $ | $ \text{Stab } A $ |
|-----|--|------------------|-------------------|--------------------|
| | $\left\{ \begin{array}{c} \text{square with diagonal } \nearrow \\ \text{square with diagonal } \nwarrow \\ \text{square with diagonal } \nearrow \\ \text{square with diagonal } \nwarrow \end{array} \right\}$ | $\{e, b\}$ | 4 | 2 |
| | $\left\{ \begin{array}{c} \text{square with diagonal } \nwarrow \\ \text{square with diagonal } \nearrow \\ \text{square with diagonal } \nwarrow \\ \text{square with diagonal } \nearrow \end{array} \right\}$ | $\{e\}$ | 8 | 1 |
| | $\left\{ \begin{array}{c} \text{square with diagonal } \nwarrow \\ \text{square with diagonal } \nwarrow \end{array} \right\}$ | $\{e, b, s, u\}$ | 2 | 4 |
| | $\left\{ \begin{array}{c} \text{square with both diagonals} \end{array} \right\}$ | $S(\square)$ | 1 | 8 |

In each case, the number of elements in the orbit multiplied by the number of elements in the stabiliser is 8, the order of the group $S(\square)$.

Solution to Exercise E166

- (a) This group action has just one orbit, namely $\{1, 2, 3, 4\}$.

Also,

$$\text{Stab } 1 = \text{Stab } 3 = \{e, s\},$$

$$\text{Stab } 2 = \text{Stab } 4 = \{e, u\}.$$

Hence, for each vertex label x ,

$$|\text{Orb } x| \times |\text{Stab } x| = 4 \times 2 = 8 = |S(\square)|.$$

- (b) The orbits of this group action are

$$\{R, T\}, \quad \{S, U\}.$$

Also,

$$\text{Stab } R = \text{Stab } T = \{e, b, r, t\},$$

$$\text{Stab } S = \text{Stab } U = \{e, b, s, u\}.$$

Hence, for each line of symmetry x ,

$$|\text{Orb } x| \times |\text{Stab } x| = 2 \times 4 = 8 = |S(\square)|.$$

- (c) The orbits of this group action are

$$\{A\}, \quad \{B, C, D\}.$$

Also,

$$\text{Stab } A = S(\triangle),$$

$$\text{Stab } B = \{e, r\},$$

$$\text{Stab } C = \{e, s\},$$

$$\text{Stab } D = \{e, t\}.$$

So for the modified triangle A we have

$$|\text{Orb } A| \times |\text{Stab } A| = 1 \times 6 = 6 = |S(\triangle)|.$$

For each other modified triangle, say x , we have

$$|\text{Orb } x| \times |\text{Stab } x| = 3 \times 2 = 6 = |S(\triangle)|.$$

(The orbits and stabilisers under the three group actions in this exercise were found in the solutions to worked exercises and exercises in Subsections 2.1 and 2.3, but it is probably quicker to find them again than to look back.)

Solution to Exercise E167

- (a) $\text{Stab } 2 = \{e, u\}$.

- (b) The left cosets of $\text{Stab } 2$ in $S(\square)$ are

$$\text{Stab } 2 = \{e, u\},$$

$$a \text{Stab } 2 = \{a \circ e, a \circ u\} = \{a, r\},$$

$$b \text{Stab } 2 = \{b \circ e, b \circ u\} = \{b, s\},$$

$$c \text{Stab } 2 = \{c \circ e, c \circ u\} = \{c, t\}.$$

- (c) We can see from Figure 49 that

e and u map 2 to 2,

a and r map 2 to 3,

b and s map 2 to 4,

c and t map 2 to 1.

So the partition of $S(\square)$ according to where its elements map 2 is

$$\{e, u\}, \quad \{a, r\}, \quad \{b, s\}, \quad \{c, t\}.$$

- (d) The partitions found in parts (b) and (c) are the same.

Solution to Exercise E168

- (a) The elements of S_3 that fix 1 are e and $(2\ 3)$, so

$$\text{Stab } 1 = \{e, (2\ 3)\}.$$

(b) The left cosets of $\text{Stab } 1$ in S_3 are

$$\text{Stab } 1 = \{e, (2\ 3)\},$$

$$(1\ 2)\text{Stab } 1 = \{(1\ 2) \circ e, (1\ 2) \circ (2\ 3)\} \\ = \{(1\ 2), (1\ 2\ 3)\},$$

$$(1\ 3)\text{Stab } 1 = \{(1\ 3) \circ e, (1\ 3) \circ (2\ 3)\} \\ = \{(1\ 3), (1\ 3\ 2)\}.$$

(c) We have

e and $(2\ 3)$ map 1 to 1,

$(1\ 2)$ and $(1\ 2\ 3)$ map 1 to 2,

$(1\ 3)$ and $(1\ 3\ 2)$ map 1 to 3.

So the partition of S_3 according to where its elements map the symbol 1 is

$$\{e, (2\ 3)\}, \quad \{(1\ 2), (1\ 2\ 3)\}, \quad \{(1\ 3), (1\ 3\ 2)\}.$$

(d) The partitions found in parts (b) and (c) are the same, as expected.

Solution to Exercise E169

The mapping f obtained from $\text{Stab } 2$ is

$$\begin{aligned} f : \text{set of left cosets of } \text{Stab } 2 &\longrightarrow \text{Orb } 2 \\ \{e, u\} &\longmapsto 2 \\ \{a, r\} &\longmapsto 3 \\ \{b, s\} &\longmapsto 4 \\ \{c, t\} &\longmapsto 1. \end{aligned}$$

Solution to Exercise E170

(a) This is a group action. We show that the group action axioms hold.

GA1 Let $g, x \in G$. Then

$$g \wedge x = gx \in G.$$

Thus axiom GA1 holds.

GA2 Let e be the identity element of G and let $x \in G$. Then

$$e \wedge x = ex = x.$$

Thus axiom GA2 holds.

GA3 Let $g, h, x \in G$. Then

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge hx \\ &= ghx \\ &= (gh) \wedge x. \end{aligned}$$

Thus axiom GA3 holds.

Hence \wedge is a group action.

(Some texts refer to this group action as the *left regular action* of a group. The proof of Cayley's Theorem given in Section 6 of Unit B3 amounts to showing that a finite group is isomorphic to the group formed by the permutations that are the effects of its elements under its left regular action. The fact that these permutations form a group follows from a result given in the optional Section 5 at the end of this unit.)

(b) This is not a group action. Axiom GA3 does not hold. If $g, h, x \in G$, then

$$g \wedge (h \wedge x) = g \wedge (xh) = xhg$$

but

$$(gh) \wedge x = xgh.$$

These two expressions are equal when $gh = hg$. This is not true in general, but it does hold when the group G is abelian.

As a particular counterexample to demonstrate that axiom GA3 does not hold, consider the group $S(\square)$ and its elements a, r and e . We have

$$a \wedge (r \wedge e) = a \wedge (e \circ r) = a \wedge r = r \circ a = u$$

but

$$(a \circ r) \wedge e = s \wedge e = e \circ s = s.$$

(c) This is a group action. We show that the group action axioms hold.

GA1 Let $g, x \in G$. Then

$$g \wedge x = xg^{-1} \in G.$$

Thus axiom GA1 holds.

GA2 Let e be the identity element of G and let $x \in G$. Then

$$e \wedge x = xe^{-1} = xe = x.$$

Thus axiom GA2 holds.

GA3 Let $g, h, x \in G$. Then

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge (xh^{-1}) \\ &= xh^{-1}g^{-1} \\ &= x(gh)^{-1} \\ &= (gh) \wedge x. \end{aligned}$$

Thus axiom GA3 holds.

Hence \wedge is a group action.

(Some texts refer to this group action as the *right regular action* of a group.)

Solution to Exercise E171

We show that the group action axioms hold.

GA1 Let $h \in H$ and let $g \in G$. Then

$$h \wedge g = hg \in G.$$

Thus axiom GA1 holds.

GA2 Let e be the identity element of H and let $g \in G$. The identity element of H is the same as the identity element of G , so

$$e \wedge g = eg = g.$$

Thus axiom GA2 holds.

GA3 Let $h_1, h_2 \in H$ and let $g \in G$. Then

$$\begin{aligned} h_1 \wedge (h_2 \wedge g) &= h_1 \wedge (h_2 g) \\ &= h_1 h_2 g \\ &= (h_1 h_2) \wedge g. \end{aligned}$$

Thus axiom GA3 holds.

Hence \wedge is a group action.

Solution to Exercise E172

We show that the group action axioms hold.

GA1 Let $g \in G$ and let $h \in H$. Then

$$g \wedge h = \phi(g) * h,$$

which is in H , since $\phi(g) \in H$. Thus axiom GA1 holds.

GA2 Let $h \in H$, and let e_G and e_H be the identity elements of (G, \circ) and $(H, *)$, respectively. Then

$$\begin{aligned} e_G \wedge h &= \phi(e_G) * h \\ &= e_H * h \end{aligned}$$

$$\begin{aligned} &(\text{since } \phi(e_G) = e_H, \text{ because } \phi \text{ is a homomorphism}) \\ &= h. \end{aligned}$$

Thus axiom GA2 holds.

GA3 Let $g_1, g_2 \in G$ and let $h \in H$. Then

$$\begin{aligned} g_1 \wedge (g_2 \wedge h) &= \phi(g_1) \wedge (\phi(g_2) * h) \quad (\text{by the definition of } \wedge) \\ &= \phi(g_1) * (\phi(g_2) * h) \quad (\text{by the definition of } \wedge) \\ &= (\phi(g_1) * \phi(g_2)) * h \quad (\text{by associativity in } (H, *)) \\ &= \phi(g_1 \circ g_2) * h \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= (g_1 \circ g_2) \wedge h \quad (\text{by the definition of } \wedge). \end{aligned}$$

Thus axiom GA3 holds.

Hence \wedge is a group action.

Solution to Exercise E173

There are four positions to be filled by a tile of a chosen colour, and there is a choice of five colours for each position. Hence by the Multiplication Principle the number of different patterns is

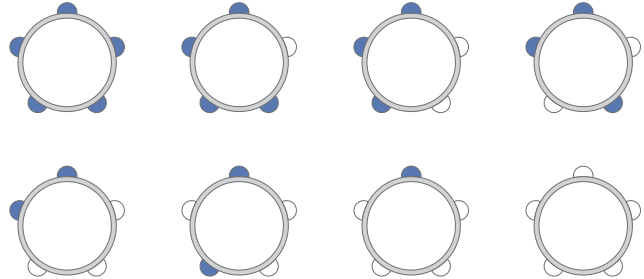
$$5 \times 5 \times 5 \times 5 = 5^4 = 625.$$

Solution to Exercise E174

(a) By the Multiplication Principle, the number of different bangles in fixed positions is

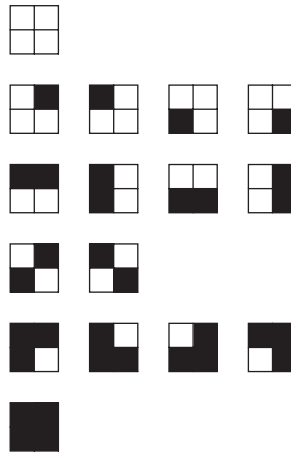
$$2 \times 2 \times 2 \times 2 \times 2 = 2^5 = 32.$$

(b) If two bangles are regarded as the same whenever one can be rotated or turned over to give the other, then there are eight different bangles, as shown below.



Solution to Exercise E175

(a) The sixteen coloured chessboards are drawn below. Those that can be rotated to give each other are drawn in the same row.



(b) If we regard two coloured chessboards as the same when one can be rotated to give the other, then there are six different coloured chessboards, namely those in the first column above.

Solution to Exercise E176

The fixed sets are

$$\text{Fix } e = \{1, 2, 3, 4\},$$

$$\text{Fix } a = \emptyset,$$

$$\text{Fix } b = \emptyset,$$

$$\text{Fix } c = \emptyset,$$

$$\text{Fix } r = \emptyset,$$

$$\text{Fix } s = \{1, 3\},$$

$$\text{Fix } t = \emptyset,$$

$$\text{Fix } u = \{2, 4\}.$$

Solution to Exercise E177

The fixed sets are

$$\text{Fix } e = \{A, B, C, D\},$$

$$\text{Fix } a = \{A\},$$

$$\text{Fix } b = \{A\},$$

$$\text{Fix } r = \{A, B\},$$

$$\text{Fix } s = \{A, C\},$$

$$\text{Fix } t = \{A, D\}.$$

Solution to Exercise E178

The fixed sets are

$$\text{Fix } e = \{A, B, C, D\},$$

$$\text{Fix } a = \emptyset,$$

$$\text{Fix } r = \{C, D\},$$

$$\text{Fix } s = \{A, B\}.$$

Solution to Exercise E179

(a) For any matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ (so $a, b \in \mathbb{R}$, $a \neq 0$),

$$\begin{aligned} & \text{Fix } \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \\ &= \left\{ (x, y) \in \mathbb{R}^2 : \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \wedge (x, y) = (x, y) \right\} \\ &= \{(x, y) \in \mathbb{R}^2 : (ax, y) = (x, y)\} \\ &= \{(x, y) \in \mathbb{R}^2 : ax = x \text{ and } y = y\} \\ &= \{(x, y) \in \mathbb{R}^2 : ax = x\}. \end{aligned}$$

(b) (i) By part (a),

$$\begin{aligned} \text{Fix } \begin{pmatrix} -1 & 5 \\ 0 & 1 \end{pmatrix} &= \{(x, y) \in \mathbb{R}^2 : -1x = x\} \\ &= \{(x, y) \in \mathbb{R}^2 : x = 0\} \\ &= \{(0, y) : y \in \mathbb{R}\}. \end{aligned}$$

So this fixed set is the y -axis.

(ii) By part (a),

$$\begin{aligned} \text{Fix } \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} &= \{(x, y) \in \mathbb{R}^2 : 1x = x\} \\ &= \mathbb{R}^2. \end{aligned}$$

So this fixed set is the whole plane \mathbb{R}^2 .

Solution to Exercise E180

- First consider the identity symmetry e in $S(\square)$. It fixes all the coloured figures in X . There are four small squares, each coloured with one of five colours, so the number of coloured figures in X is 5^4 . Hence

$$|\text{Fix } e| = 5^4.$$

- Now consider the symmetry a . The coloured figures in X fixed by a are those in which the four small squares are all the same colour. Hence

$$|\text{Fix } a| = 5.$$

By a similar argument,

$$|\text{Fix } c| = 5.$$

- Next consider the symmetry b . The coloured figures in X fixed by b are those in which each small square is the same colour as the diagonally opposite small square. There are two pairs of diagonally opposite small squares and five choices for the colour of each pair, so

$$|\text{Fix } b| = 5^2.$$

- Next consider the symmetry r . The coloured figures in X fixed by r are those in which each small square is the same colour as the square next to it horizontally. There are two pairs of small squares next to each other horizontally and five choices for the colour of each pair, so

$$|\text{Fix } r| = 5^2.$$

By a similar argument,

$$|\text{Fix } t| = 5^2.$$

- Next consider the symmetry s . The coloured figures in X fixed by s are those in which the top right small square is the same colour as the bottom left small square. Hence there are three colour choices to be made – the single colour of the top right and bottom left small squares, and the colour of each of the other two small squares. Each colour choice is from five colours, so

$$|\text{Fix } s| = 5^3.$$

By a similar argument,

$$|\text{Fix } u| = 5^3.$$

The sizes of the fixed sets for this group action are summarised below.

| Symmetry g | $ \text{Fix } g $ |
|--------------|-------------------|
| e | 5^4 |
| a | 5 |
| b | 5^2 |
| c | 5 |
| r | 5^2 |
| s | 5^3 |
| t | 5^2 |
| u | 5^3 |

(Notice that, as expected, symmetries that are conjugate in $S(\square)$ have fixed sets of the same size. The conjugacy classes of $S(\square)$, found in Worked Exercise E28 in Subsection 2.3 of Unit E2, are

$$\{e\}, \quad \{a, c\}, \quad \{b\}, \quad \{r, t\}, \quad \{s, u\}.)$$

Solution to Exercise E181

Each of the fixed sets in Exercise E180 has size c^k where c is the number of colours and k is the number of colour choices to be made. If we change the number of colours from 5 to 4, then a fixed set of size 5^k changes to a fixed set of size 4^k . So the sizes of the fixed sets for the group action with four colours are as given below.

| Symmetry g | $ \text{Fix } g $ |
|--------------|-------------------|
| e | 4^4 |
| a | 4 |
| b | 4^2 |
| c | 4 |
| r | 4^2 |
| s | 4^3 |
| t | 4^2 |
| u | 4^3 |

Solution to Exercise E182

We can label the figure as follows.

| | |
|---|---|
| 2 | 1 |
| 3 | 4 |

This gives the following.

| Symmetry g | Permutation | Number of cycles | $ \text{Fix } g $ |
|--------------|----------------|------------------|-------------------|
| e | $(1)(2)(3)(4)$ | 4 | 5^4 |
| a | $(1\ 2\ 3\ 4)$ | 1 | 5 |
| b | $(1\ 3)(2\ 4)$ | 2 | 5^2 |
| c | $(1\ 4\ 3\ 2)$ | 1 | 5 |
| r | $(1\ 2)(3\ 4)$ | 2 | 5^2 |
| s | $(1\ 3)(2)(4)$ | 3 | 5^3 |
| t | $(1\ 4)(2\ 3)$ | 2 | 5^2 |
| u | $(1)(3)(2\ 4)$ | 3 | 5^3 |

(Your permutations may be different if you chose a different labelling of the squares.)

Solution to Exercise E183

We are regarding two coloured headscarves as the same if one can be rotated or reflected to give the other. So we consider the action of the group $S(\square)$ on the set of all possible coloured headscarves in fixed positions. The sizes of the fixed sets for this group action, found in Exercise E182 (and Exercise E180) in the previous subsection, are shown below.

| Symmetry g | $ \text{Fix } g $ |
|--------------|-------------------|
| e | 5^4 |
| a | 5 |
| b | 5^2 |
| c | 5 |
| r | 5^2 |
| s | 5^3 |
| t | 5^2 |
| u | 5^3 |

By the Counting Theorem, the number of orbits is

$$\begin{aligned}
& \frac{1}{8}(5^4 + 5 + 5^2 + 5 + 5^2 + 5^3 + 5^2 + 5^3) \\
&= \frac{1}{8}(5^4 + 2 \times 5 + 3 \times 5^2 + 2 \times 5^3) \\
&= \frac{5}{8}(5^3 + 2 + 3 \times 5 + 2 \times 5^2) \\
&= \frac{5}{8}(125 + 2 + 15 + 50) \\
&= \frac{5}{8} \times 192 \\
&= 120.
\end{aligned}$$

Thus 120 different headscarves can be made.

Solution to Exercise E184

Consider the action of the group $S(\square)$ on the set of all possible coloured headscarves in fixed positions. The sizes of the fixed sets for this group action are the same as those given in the solution to Exercise E183, but with 4 colours replacing 5 colours (as you saw in Exercise E181 in the previous subsection).

Thus the sizes of the fixed sets are as follows.

| Symmetry g | $ \text{Fix } g $ |
|--------------|-------------------|
| e | 4^4 |
| a | 4 |
| b | 4^2 |
| c | 4 |
| r | 4^2 |
| s | 4^3 |
| t | 4^2 |
| u | 4^3 |

By the Counting Theorem, the number of orbits is

$$\begin{aligned}
& \frac{1}{8}(4^4 + 4 + 4^2 + 4 + 4^2 + 4^3 + 4^2 + 4^3) \\
&= \frac{1}{8}(4^4 + 2 \times 4 + 3 \times 4^2 + 2 \times 4^3) \\
&= \frac{1}{2}(4^3 + 2 + 3 \times 4 + 2 \times 4^2)
\end{aligned}$$

$$\begin{aligned}
&= 2 \times 4^2 + 1 + 3 \times 2 + 4^2 \\
&= 32 + 1 + 6 + 16 \\
&= 55.
\end{aligned}$$

Thus 55 different headscarves can be made if only four colours are allowed.

Solution to Exercise E185

We are regarding two coloured chessboards as the same if one can be rotated to give the other. So we consider the action of the group $S^+(\square)$ on the set of all 2^4 coloured 2×2 chessboards in fixed positions.

We can label the squares of the chessboard as follows.

| | |
|---|---|
| 2 | 1 |
| 3 | 4 |

Thus the sizes of the fixed sets are as follows.

| Symmetry g | Permutation | Number of cycles | $ \text{Fix } g $ |
|--------------|----------------|------------------|-------------------|
| e | $(1)(2)(3)(4)$ | 4 | 2^4 |
| a | $(1\ 2\ 3\ 4)$ | 1 | 2 |
| b | $(1\ 3)(2\ 4)$ | 2 | 2^2 |
| c | $(1\ 4\ 3\ 2)$ | 1 | 2 |

(Your permutations may be different if you chose a different labelling of the squares.)

(The sizes of the fixed sets are the same as the first four sizes of fixed sets given in the solutions to Exercises E183 and E184, but with two colours replacing five or four colours, respectively. There are only four fixed sets to be considered here, rather than eight, because we are considering the action of the group $S^+(\square)$ rather than that of the whole symmetry group $S(\square)$.)

By the Counting Theorem, the number of orbits is

$$\begin{aligned}
& \frac{1}{4}(2^4 + 2 + 2^2 + 2) = \frac{1}{4}(16 + 2 + 4 + 2) \\
&= \frac{1}{4} \times 24 \\
&= 6.
\end{aligned}$$

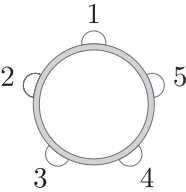
Thus there are 6 different coloured chessboards.

This is the same answer as found in Exercise E175.

Solution to Exercise E186

We are regarding two coloured bangles as the same if one can be rotated or turned over to give the other. So we consider the action of the group $S(\diamond)$ on the set of all possible coloured bangles in fixed positions. As there are two colours, there are 2^5 coloured bangles in fixed positions.

We can label the beads as shown below.



The sizes of the fixed sets for this group action are as given below. (For convenience, we collect together symmetries of the same geometric type.)

| Symmetry g | Example permutation | Number of cycles | $ \text{Fix } g $ |
|-----------------------------------|---------------------|------------------|-------------------|
| e | $(1)(2)(3)(4)(5)$ | 5 | 2^5 |
| 2 rotations, through $\pm 2\pi/5$ | $(1\ 2\ 3\ 4\ 5)$ | 1 | 2 |
| 2 rotations, through $\pm 4\pi/5$ | $(1\ 3\ 5\ 2\ 4)$ | 1 | 2 |
| 5 reflections | $(1)(2\ 5)(3\ 4)$ | 3 | 2^3 |

By the Counting Theorem, the number of orbits is

$$\begin{aligned} &\frac{1}{10}(2^5 + 2 \times 2 + 2 \times 2 + 5 \times 2^3) \\ &= \frac{1}{10}(32 + 4 + 4 + 40) \\ &= \frac{1}{10} \times 80 \\ &= 8. \end{aligned}$$

Thus eight different coloured bangles can be made. This is the same answer as found in Exercise E174(b).

Solution to Exercise E187

We consider the action of the group $S^+(\square) = \{e, a, b, c\}$ on the set of all possible coloured chessboards in fixed positions.

- The identity symmetry e fixes all the coloured chessboards. There are 16 small squares, each coloured one of two colours, so the number of coloured chessboards is 2^{16} . Hence

$$|\text{Fix } e| = 2^{16}.$$

- Now consider the symmetry a . The coloured chessboards fixed by a are those in which each square is the same colour as the three squares onto which it is mapped under successive quarter turns. There are 2^4 different ways to colour one quarter of such a chessboard, and this colouring determines the colours of the squares in each of the other quarters of the chessboard. Thus

$$|\text{Fix } a| = 2^4.$$

By a similar argument,

$$|\text{Fix } c| = 2^4.$$

- Finally consider the symmetry b . The coloured chessboards fixed by b are those in which each square is the same colour as the square onto which it is mapped under a half turn. There are 2^8 different ways to colour one half of such a chessboard, and this colouring determines the colours of the squares in the other half. Thus

$$|\text{Fix } b| = 2^8.$$

By the Counting Theorem, the number of orbits is

$$\begin{aligned} \frac{1}{4}(2^{16} + 2 \times 2^4 + 2^8) &= \frac{1}{4}(2^{16} + 2^5 + 2^8) \\ &= \frac{1}{4} \times 2^5(2^{11} + 1 + 2^3) \\ &= 2^3(2^{11} + 2^3 + 1). \end{aligned}$$

This is the number of different coloured chessboards.

(The number $2^3(2^{11} + 2^3 + 1)$ is a little time-consuming to evaluate without a calculator. A calculator shows that its value is 16 456.)

Solution to Exercise E188

To determine the number of coloured cubes when only two colours are available, we rework the calculation in the solution to Worked Exercise E79, changing the number of colours from 3 to 2 wherever it occurs. This gives the answer

$$\begin{aligned}
 & \frac{1}{24}(2^6 + 6 \times 2^3 + 3 \times 2^4 + 8 \times 2^2 + 6 \times 2^3) \\
 &= \frac{1}{24} \times 2^2(2^4 + 6 \times 2 + 3 \times 2^2 + 8 + 6 \times 2) \\
 &= \frac{1}{6}(16 + 12 + 12 + 8 + 12) \\
 &= \frac{1}{6} \times 60 \\
 &= 10.
 \end{aligned}$$

So there are 10 different coloured cubes if only two colours are available.

Solution to Exercise E189

(a) The homomorphism ϕ is as follows, where e and i are the identity elements of $(S(\square), \circ)$ and $(\text{Sym } X, \circ)$, respectively.

$$\begin{aligned}
 \phi : (S(\square), \circ) &\longrightarrow (\text{Sym } X, \circ) \\
 e &\longmapsto i \\
 a &\longmapsto (A \ B \ C) \\
 b &\longmapsto (A \ C \ B) \\
 c &\longmapsto i \\
 d &\longmapsto (A \ B \ C) \\
 f &\longmapsto (A \ C \ B) \\
 r &\longmapsto (B \ C) \\
 s &\longmapsto (A \ B) \\
 t &\longmapsto (A \ C) \\
 u &\longmapsto (B \ C) \\
 v &\longmapsto (A \ B) \\
 w &\longmapsto (A \ C)
 \end{aligned}$$

(b) The homomorphism ϕ is as follows, where e and i are the identity elements of $(S(\square), \circ)$ and $(\text{Sym } X, \circ)$, respectively.

$$\begin{aligned}
 \phi : (S(\square), \circ) &\longrightarrow (\text{Sym } X, \circ) \\
 e &\longmapsto i \\
 a &\longmapsto (J \ K)(L \ M) \\
 b &\longmapsto i \\
 c &\longmapsto (J \ K)(L \ M) \\
 d &\longmapsto i \\
 f &\longmapsto (J \ K)(L \ M)
 \end{aligned}$$

$$\begin{aligned}
 r &\longmapsto (J \ L)(K \ M) \\
 s &\longmapsto (J \ M)(K \ L) \\
 t &\longmapsto (J \ L)(K \ M) \\
 u &\longmapsto (J \ M)(K \ L) \\
 v &\longmapsto (J \ L)(K \ M) \\
 w &\longmapsto (J \ M)(K \ L)
 \end{aligned}$$

Solution to Exercise E190

(a) For the group action in Exercise E189(a), the subsets in the partition of $S(\square)$ and their corresponding permutations of X are as shown below.

| Subset in partition of $S(\square)$ | Corresponding permutation of X |
|-------------------------------------|----------------------------------|
| $\{e, c\}$ | i |
| $\{a, d\}$ | $(A \ B \ C)$ |
| $\{b, f\}$ | $(A \ C \ B)$ |
| $\{r, u\}$ | $(B \ C)$ |
| $\{s, v\}$ | $(A \ B)$ |
| $\{t, w\}$ | $(A \ C)$ |

(b) For the group action in Exercise E189(b), the subsets in the partition of $S(\square)$ and their corresponding permutations of X are as shown below.

| Subset in partition of $S(\square)$ | Corresponding permutation of X |
|-------------------------------------|----------------------------------|
| $\{e, b, d\}$ | i |
| $\{a, c, f\}$ | $(J \ K)(L \ M)$ |
| $\{r, t, v\}$ | $(J \ L)(K \ M)$ |
| $\{s, u, w\}$ | $(J \ M)(K \ L)$ |

(Notice that in each of parts (a) and (b) the listed permutations of X form a subgroup of $\text{Sym } X$, as expected in view of Corollary E72(a).)

It also follows from the above and Corollary E72(b) that $\{e, c\}$ and $\{e, b, d\}$ are normal subgroups of $S(\square)$.)

Solution to Exercise E191

We check the group action axioms.

GA1 Let $g \in G$ and let $x \in X$. We have to show that $g \wedge x \in X$. Now

$$\begin{aligned} g \wedge x &= (\phi(g))(x) \quad (\text{by the definition of } \wedge) \\ &\in X \quad (\text{since } \phi(g) \text{ is a permutation of } X). \end{aligned}$$

Thus axiom GA1 holds.

GA2 Let e be the identity element of $(G, *)$ and let $x \in X$. We have to show that $e \wedge x = x$. Let i be the identity element of $(\text{Sym } X, \circ)$; that is, i is the identity permutation of X . Now

$$\begin{aligned} e \wedge x &= (\phi(e))(x) \quad (\text{by the definition of } \wedge) \\ &= i(x) \\ &\quad (\text{since } \phi(e) = i, \text{ as } \phi \text{ is a homomorphism}) \\ &= x. \end{aligned}$$

Thus axiom GA2 holds.

GA3 Let $g, h \in G$ and let $x \in X$. We have to show that $g \wedge (h \wedge x) = (g * h) \wedge x$. Now

$$\begin{aligned} g \wedge (h \wedge x) &= g \wedge (\phi(h)(x)) \quad (\text{by the definition of } \wedge) \\ &= \phi(g)(\phi(h)(x)) \quad (\text{by the definition of } \wedge) \\ &= (\phi(g) \circ \phi(h))(x) \\ &\quad (\text{by the definition of function composition}) \\ &= (\phi(g * h))(x) \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= (g * h) \wedge x \quad (\text{by the definition of } \wedge). \end{aligned}$$

Thus axiom GA3 holds.

Since the three group action axioms hold, \wedge is a group action.

Acknowledgements

Grateful acknowledgement is made to the following sources.

Cover image: © Mark Owen

Unit E1

Church bells (Subsection 4.3): Courtesy of Tim Lowe

Bell ringers (Subsection 4.3): Courtesy of Tim Lowe

Unit E2

Otto Hölder (Subsection 1.1): From:

<http://www-history.mcs.st-andrews.ac.uk>

Niels Henrik Abel (Subsection 1.3): Municipal Archives of Trondheim.

This file is licensed under Creative Commons Attribution 2.0 Generic.

<http://creativecommons.org/licenses/by/2.0/>

Daniel Gorenstein (Subsection 1.3): From:

<http://www-history.mcs.st-and.ac.uk>

Michael Aschbacher (Subsection 1.3): Jan-Olav Wedin

Stephen Smith (Subsection 1.3): Courtesy of Professor Emeritus

Stephen D. Smith

Unit E3

Lev Semyonovich Pontryagin (Subsection 2.2): From:

<http://www-history.mcs.st-andrews.ac.uk>

Bartel van der Waerden (Subsection 3.2): From: Wikimedia.org

Emmy Noether (Subsection 3.2): Mathematical Association. This file is

licensed under the Creative Commons Attribution - No Derivatives Licence

<http://creativecommons.org/licenses/by-nd/2.0>

Unit E4

Ferdinand Georg Frobenius (Subsection 4.3): Ullstein Bild / Getty Images

Augustin-Louis Cauchy (Subsection 4.3): Library of Congress Prints and
Photographs Division / Wikipedia

George Pólya (Subsection 4.3): From:

<http://www-history.mcs.st-and.ac.uk>

Every effort has been made to contact copyright holders. If any have been inadvertently overlooked the publishers will be pleased to make the necessary arrangements at the first opportunity.

Index

\wedge 294, 297

Abel, Niels Henrik 127

abelian (commutative) group 7

action of a group *see* group action

additive group 36

cosets in 69

additive notation 36

A_n , alternating group 18, 78

conjugacy classes of A_5 160

Aschbacher, Michael 128

associativity 4

automorphism 213

bangle problem 353

solution of 368

bell ringing 71

benzene, the Counting Theorem applied to 374

Betti, Enrico 109

binary operation 4

blocking of a group table 109–110

Burnside's Lemma 367

Burnside, William 109, 367

Cancellation Laws 11

Cauchy, Augustin-Louis 367

Cayley table 8

characterisation of a normal subgroup 148, 161

chessboard problem 354

solution of 370

classification of finite simple groups 128

closure (group axiom) 4

Cole, Frank Nelson 62

coloured figure 309

commutative (abelian) group 7

concise multiplicative notation 52

conjugacy 134

and geometric type 164

and normal subgroups 147, 155

as an equivalence relation 140

in a symmetric group 129–133

in a symmetry group 166–168, 174

in subgroups of groups 144–145

conjugacy class 138, 141

and normal subgroups 156

finding 141

in a symmetry group 175

number of elements in 146, 350

of $S(\square)$ 164

of $S(\triangle)$ 164

of an abelian group 144

conjugate element 134, 135

in a symmetry group 168

order of 137

conjugate permutation 129, 131, 133

finding (renaming method) 129

conjugate subgroup 151–153

in a matrix group 180

order of 154

conjugating element 134

conjugating permutation 129

finding 132

conjugation as a group action 348

coset 52, 79

in an additive group 69

left 53, 55

method for finding 59, 67

properties of 57

of the kernel of a homomorphism 261, 262

right 62, 64

method for finding 64, 67

properties of 64

counting problem 352

Counting Theorem 365

proof of 376

cube problem 356

solution of 372

cycle form 13

cycle of a permutation 13

as a composite of transpositions 16

disjoint 13

cycle structure 18

cyclic group 43

finite 44

subgroups of 44

cyclic subgroup 41, 43

- de Bruijn, Nicolaas Govert 367
- Dedekind, Richard 109
- determinant 28
- diagonal matrix 31
- dihedral group 126
- direct symmetry 21
- disjoint cycles 13
- disjoint sets 55

- equilateral triangle, symmetry group of 20
 - subgroups of 25
- equivalence class 56
- equivalence relation 56
- even permutation 17

- factor group 108, *see also* quotient group
- faithful group action 300
- figure in \mathbb{R}^2 or \mathbb{R}^3 19
 - coloured 309
- finite group 7
- finite order of a group element 38
- finite simple groups, classification of 128
- First Isomorphism Theorem 266
- fixed point set of a symmetry 171, 358
- fixed set of a group element 356
 - finding the size of 360
 - permutation method for 363
 - under a group action on \mathbb{R}^2 358
- $\text{Fix } g$ 171, 356
- fixing of an element 296
- fractional part of a real number 6
- Frobenius, Ferdinand Georg 367

- Galois, Évariste 127
- general linear group 27, 29
- generator 43
- $\text{GL}(n)$ 27
- $\text{GL}(2)$ 29
- Golomb, Solomon 367
- Gorenstein, Daniel 128

- group 4
 - abelian/non-abelian 7
 - additive 36
 - alternating 18, 78
 - cyclic 43
 - general linear 27, 29
 - isomorphic 45, 46, 48
 - multiplicative 36
 - of prime order 51
 - of symmetries 303
 - simple 124
 - standard small 50
 - symmetric 18
 - symmetry 19
- group action 297, 302, 378
 - and groups of permutations 378–383
 - and left cosets of a stabiliser under 343
 - as a homomorphism 383
 - faithful 300
 - left/right 341–342
 - natural 302
 - of a group of numbers 311–313
 - of a group of symmetries 309–311
 - of a matrix group 314–317
 - on a group 347
- group action axioms 297
- group axioms 4
 - checking 5–6, 8
- group table 8
 - properties of 12

- Hölder, Otto 109
- homomorphism 222
 - and group actions 351
 - and quotient groups 266, 272
 - effect on the order of an element 237
 - linear transformation as 230
 - one-to-one 251
 - preservation of composites under 231–233
 - preservation of conjugates under 238
 - preservation of inverses under 234
 - preservation of powers under 235
 - preservation of the identity under 233
 - properties of 231–238, 245
 - structure-preserving properties of 243–245
 - trivial 230
- homomorphism property 222

- identity element (identity) 4
 - in a subgroup 23
 - uniqueness of 11
- identity function 296
- identity matrix 28
- identity permutation 18, 379
- identity symmetry 19
- image
 - of a coloured figure 309
 - of a figure 304
- image (image set) of a homomorphism 239, 266
 - finding 253, 258, 259
 - order of 271
 - properties of 242, 245
- index laws for group elements 38
- index of a subgroup 68
- indirect symmetry 21
- infinite group 7
- infinite index 68
- infinite order of a group element 38
- inverse element (inverse) 4
 - in a subgroup 23
 - of a permutation 15
 - order of 39
 - uniqueness of 11
- inverse matrix 28
- invertible matrix 28
- isomer, chemical 374
- isometry 19
- isomorphic groups 45, 46, 48, 214
- isomorphism 46, 48, 209, 214
 - inverse of 219
 - of cyclic groups 220
- isomorphism class 49
 - for groups of orders 1 to 8 50
- Jordan, Camille 109, 127
- kernel of a homomorphism 247, 249, 266
 - and normal subgroups 252
 - cosets of 261, 262
 - finding 253, 255, 259
 - order of 271
 - properties of 249–251
- Klein four-group 50
- Klein, Felix 62
- Lagrange's Theorem 27, 61
 - and group actions 349
- least residue 228
- left coset 53, 55
 - method for finding 59, 67
 - properties of 56–57
- left cosets of a stabiliser 341
- left group action 341
- left regular action 395
- length of a cycle 13
- linear transformation 230
- lower triangular matrix 30
- mapping 46
- matrix 27
 - diagonal 31
 - lower triangular 30
 - upper triangular 31
- Miller, George Abram 62
- $M_{m,n}$ 27
- multiple of a group element 37
- Multiplication Principle 352
- multiplicative group 36
- multiplicative notation 36
 - concise 52
- natural action of a group 302
- Netto, Eugen 62
- Neumann, Peter M. 367
- Noether, Emmy 272
- non-abelian group 7
- non-cyclic group 43
- non-isomorphic groups 214
- normal subgroup 76–79
 - and conjugacy classes 156
 - and conjugates 147
 - characterisations of 148, 161
 - finding 160
 - in a matrix group 185
 - using to form a quotient group 108
- normality of a subgroup 147
- odd permutation 17
- orbit 318
 - finding 319, 323
 - of a group action 323
 - of a group action on \mathbb{R}^2 325
 - of a set element 318
- Orbit–Stabiliser Theorem 340
 - proof of 347

- Orb x 318
- order
 - of a group 7
 - of a group element 38, 40
 - of a permutation 41
 - of a subgroup 27
- Pólya Enumeration Theorem 375
- Pólya, George 375
- parity of a permutation 17
- partition 55
- permutation 12, 301
 - conjugate 129
 - conjugating 129
 - composing 14
 - cycle form of 13
 - even/odd 17
 - finding the inverse of 15
 - group of 12
 - order of 41
 - parity of 17–18
 - two-line form of 12
- permutation group 18
- permuting the elements of a set 301
- plane figure 19
- Pontryagin, Lev Semyonovich 252
- power of a group element 37, 40
- preservation (under a homomorphism) of
 - composites 215, 231
 - conjugates 238
 - inverses 234
 - powers 235
 - the identity 233
- prime order, group of 51
- quaternion group 50
- quotient group 108
 - and homomorphisms 266
 - infinite 120, 272
 - of \mathbb{R} 120
 - of \mathbb{Z} 115
 - of a finite group 112–115
 - of an infinite group 115–123
- rectangle, symmetry group of 20, 21
- Redfield, John Howard 375
- reflexive property (reflexivity) 56
- relation 55
- renaming method 129
- right coset 62, 64
 - method for finding 64, 67
 - properties of 64
- right group action 342
- right regular action 395
- Ruffini, Paolo 127
- $S(\triangle)$ 20, 21
 - conjugacy classes of 164
 - subgroups of 25
- $S(\square)$ 20, 21
 - conjugacy classes of 164
 - subgroups of 25
- $S(\square)$ 20, 21
- $S(\text{cuboid})$ 19
- $S(\text{tet})$ 19
- $S(F)$ 19
- $S^+(F)$ 24
- S_n (symmetric group) 18
 - subgroups of 26
- self-inverse element 9
 - subgroup generated by 43
- set composition 100
 - in an additive group 101
 - of cosets of a normal subgroup 104, 108
- simple group 124
- $SL(n)$ 32
- Smith, Stephen 128
- solid figure 19
- special linear group 32
- square, symmetry group of 20, 21
- stabiliser 330, 333
 - of an element of \mathbb{R}^2 335
- $\text{Stab } x$ 330
- standard groups of numbers
 - finite 10
 - infinite 7
- standard small groups 50
- subgroup 22
 - conjugate 151–153
 - cyclic 41, 43
 - normal 76–79
 - order of 27
 - trivial 23
- subgroup properties 23
- subgroup test 23

- symmetric group
 - S_n 18
 - subgroups of 26
 - on any set (finite or infinite) 379
- symmetric property (symmetry) 56
- symmetry group 19
 - $S(\triangle)$, $S(\square)$ and $S(\square)$ 20, 21
- symmetry of a figure 19
 - direct/indirect 21
- $\text{Sym } X$ 378, 379
- transitive property (transitivity) 56
- transposition 16
- triangle, equilateral, symmetry group of 20, 21
- trivial homomorphism 230
- trivial subgroup 23
- two-line form of a permutation 12
- (U_n, \times_n) 10
- upper triangular matrix 31
- V (Klein four-group) 50
- van der Waerden, Bartel 272
- wedge symbol 294, 297
- $(\mathbb{Z}_n, +_n)$ 10, 44
 - subgroups of 45
- $(\mathbb{Z}_p^*, \times_p)$ 10

